"Bridging the Gap from Theory to Outcomes" *Volume 3, Issue 13, Summer 2009*

In This Issue

How to Keep Your Email Inbox Under Control 2
Is Your Email Businesslike or Brusque? 3
Microsoft: 97% of Emails are Spam..... 4
Email Management: The Good, the Bad and the Ugly 5
Clouds on the Information Horizon: How to Avoid the Storm..... 7
Checklist for Evaluating Cloud-Based Initiatives..... 11
Why Your Email Inbox is Not a Good To-Do List 12
Records and Information Management Resources 13
Upcoming Training Opportunities 13

TIPS AND TRICKS

Process your inbox from the top down, making quick and immediate decisions. Start with the top item in your inbox, and make an immediate decision. Don't skip over it or put it back in or delay the decision. Here are your choices: delete, delegate to someone else, do it immediately (if it takes 2 minutes or less), or defer it for later (add it to your to-do list). In all cases, don't leave the item in your inbox. Delete or file it. Work your way down through each item until your inbox is empty. Note: if you have hundreds of items in your inbox, it might be good to toss them all into a folder to be processed later (and schedule a couple hours to do that), and then start this process with all new items from that point on.

—Zenhabits—Simple Productivity
http://zenhabits.net

Mary Colak, CMC

Email seems to be the biggest '"tripping" point for many people. It still amazes me when people tell me that they find it "easier" to keep all of their emails in their inbox rather than clearing emails daily.

I don't believe that it is easier to retrieve old email from an inbox shrouded by hundreds, if not thousands, of other emails. Retrieving opened email that has been sorted and filed in appropriate folders and files is much more productive.

In its July/August 2009 Information Management Journal, ARMA International reported that employees spend about 3.5 hours per week every year searching for information they can't find. This includes email. Assuming an average rate of pay of $30.00 per hour, this is about $5,500 wasted productivity per employee per year. Multiply that by a few hundred or several thousand employees and, well, you can see how that waste certainly adds up!

I have had many queries over the past couple of months about email and, specifically, how to manage email, so I am devoting most of this newsletter to that topic.

I appreciate receiving your comments and suggestions, so please continue sending them! My email address is: mary@rimsolutions.ca. I make every effort to answer all mail promptly (unless I'm on vacation!).

Best wishes,

Mary Colak, cmc

How to Keep Your Email Inbox Under Control

David Silverman, May 11, 2009 in www.harvardbusiness.org.

Note—the opinions expressed in this article by David Silverman do not necessarily reflect the opinions of RIM Management Consultants. The article is merely provided as another way to look at managing one's email. After all, we're all unique in our approaches to email management, but the key is to find a system/method that works for you so that you are productive with your email.

A reader recently asked me, "How do you deal with an incredibly full inbox that makes you feel like a jerk?"

I'm happy the question asks, "how do *you* deal." An inbox is as personal a space as an underwear drawer—we all have one and are all embarrassed by both its organization and contents. Thus to tell someone how to manage their inbox could be perceived as an intrusion into their undergarments.

And that would be inappropriate.

What *is* appropriate to share is my own principles of inbox management:

1. **No scrolling.** The inbox is my task list. I can fit about 20 emails in the message viewer in Apple Mail, which means 20 tasks. Any more than that and I feel like I'm losing control. Nothing spurs me to action like the need to get rid of the scroll bars.
2. **Read, take action, and delete or save.** Small task or big one, if it's in the inbox, I do it. If not, it doesn't exist (as my wife can tell you about any time we make vacation plans).
3. **If it's a task for someone else, file it.** I find it hard enough to keep track of my own to-dos. Keeping tabs on other people's through emails in my inbox would triple the number of messages and lead me down the road of micromanagement via the dreaded forwarded email that begins with, "Hey, have you had a chance to look at this yet?"
4. **One email per topic.** If there's a chain of email on a topic, only the most recent gets to sit in my inbox. Everything else is filed.
5. **Save everything that isn't pure junk.** Which email is important and which is not? It can be hard to tell. The email with a dancing banana? Probably safe to toss. But will I need an email with the details of my cat's last tooth cleaning? Possibly. And with gigabytes of storage on my hard drive, it's as easy to save as not.
6. **Have very few file folders.** Almost everything saved goes into a folder called "saved." With too many folders, the time it takes me to sort and organize emails is prohibitive — and it often requires just as much time on the other end to locate the message I want. Instead, I rely on my email's search feature. (Just now, it was easy to uncover from my "sent mail" folder the information that veterinary dental work costs a terrifying $450 per feline.)
7. **Daily scrubbing.** I brush my teeth twice a day. And every day, I run through every email in my inbox to see if I can get rid of it.
8. **Nothing older than a month.** I'll let something smolder in the inbox for up to a month if I'm not sure what to do with it — or if it's something I'd like to do, but never seem to get to. But after a month, it's clear I've got to do it or delete it.

What are your tips for email management?

■

David Silverman is the author of *Typo: The Last American Typesetter or How I Made and Lost 4 Million Dollars* (Soft Skull Press, 2007). He has worked at brand-new start-ups, Fortune 500 companies, and a few places in between. A business writing teacher, he grapples with the way we use words at work—to make it easier for the rest of us. If you have questions about how to manage a problem at work related to communication, please contact David at dsilverman [at] harvardbusiness [dot] org.

Is Your Email Businesslike or Brusque?

David Silverman, May 22, 2009 in www.harvardbusiness.org.

A reader writes with the following query:

"I manage 15 staff who are scattered about. I email them since it's the easiest way for me to communicate with all of them at the same time. Often my emails are very short and to the point. It's business. Two staff see that as my being harsh and have no problem letting me know that. Example: "Would you please update these primary care providers in the database, including addresses and phone numbers?"

Six days later, I sent the following email as follow up to my initial request: "I would like this taken care of by Thursday this week. If you are having trouble getting this done, please let me know."

In return, my employee sent me a lengthy 4 paragraph response on how insulted she was by my follow up email. I would like your opinion."

On the one hand, the employee's response was out of line. What was he or she hoping to achieve? It didn't get the project done and it almost certainly didn't improve your relationship. I'd go as far as to say it's justified for you to reprimand someone for aggressive behavior like that.

But that's me speaking as a boss (or customer) who's sent similar emails to yours. I've also been the recipient—and felt rising anger every time one of my bosses sent an email beginning with, "Please provide the revised presentation..."

Perhaps unexpectedly, it was the "please" that drove me over the edge. And while I didn't fire off a petulant four-paragraph response, I did seethe quietly. And, more importantly, I didn't feel very much like "providing the revised presentation."

Anyone who's ever been part of an online "flame war" has had the experience of a tiny "e-mole" becoming a mountain. (And yes, I am also shocked that I would attempt such a terrible pun.) Studies have shown that readers add (or invent) emotional bias that is often counter to your intent as the sender.

In this case, all of the niceties you *thought* you were writing ended up sounding very different in the mind of your employee.

In the echo chamber of the employee's mind, and the absence of other cues from you, "I would like" was probably heard as a passive-aggressive demand, if not a derisive sneer. "If you are having trouble," was meant as "I'm here to help," but interpreted as "I think you're a dolt for taking 6 days to do a minor task." The length of your email also compounded the emotional dissonance. You thought of it as just a quick note on a task, but your brevity came across as curt.

Lastly, the form of communication itself (email) could be interpreted as, "Just so you know, I'm documenting your incompetence."

Ouch, right?

Here are some suggestions for preventing this next time:

1. **You could call.** Your goal is to check the progress of the task and give the employee a chance to respond with questions—a call could accomplish this while allowing both of you to hear each other's tone of voice. Since you say at least two of your staff find your emails harsh, this could be the easiest solution.

2. **Include deadlines when you first make a request.** If you don't have time to call, or if time zones make calling a hassle, email can still work if you revise your initial request to include a due date, or, for a bigger project, a due date for a status update. By giving a date, your follow-up won't feel as aggressive and your employee will be less likely to take it personally. Deadlines will also help your staff prioritize — perhaps rendering follow-ups unnecessary.

See Businesslike on page 4

Businesslike, continued from page 3

3. **Be conversational.** Even if the first email was unchanged, the second email could be written to avoid a blow up. You don't need lots of smiley faces or exclamation points. You just need to write the way you might actually talk. For example, your second email could read: "Hi Cindy, just following up on the email below—can you let me know how far along the task is? I was hoping we could have this by the meeting on Thursday, is that a possibility?"
4. **Use the passive voice.** It doesn't make for great writing, but it can help you avoid sounding accusatory—and it sounds like your employee felt accused.
5. **Share your train of thought.** If I know *why* you emailed me 37 spreadsheets and asked for me to combine them by Tuesday, it allows me to be part of the process rather than feel like a cog being dumped on.

To handle the situation as it is now, call. Let your employee know you meant no disrespect, and that your goal, and theirs, was and is to get the job done. And let them know that the I'm-an-emotional-person-and-you-hurt me email has no place at work.

Lastly, I'd like to use this as an opportunity to repeat why I think even the "simplest" emails need to be revised with care. It takes time and thought to ensure you don't give the wrong emotional cues.

Let's open this up to my readers and get you some more opinions. Does anyone have other advice? Do you disagree with the recommendations I've proposed? ■

David Silverman is the author of *Typo: The Last American Typesetter or How I Made and Lost 4 Million Dollars* (Soft Skull Press, 2007). He has worked at brand-new start-ups, Fortune 500 companies, and a few places in between. A business writing teacher, he grapples with the way we use words at work—to make it easier for the rest of us. If you have questions about how to manage a problem at work related to communication, please contact David at dsilverman [at] harvardbusiness [dot] org.

Microsoft: 97% of Emails are Spam

Source: Information Management Journal, July/August 2009

According to a 2008 Microsoft security report, only 3% of emails sent are wanted; 97% are spam messages that may contain viruses or other malicious software.

The report also found the global ratio of infected machines was 8.6 for every 1,000 uninfected machines.

Ed Gibson, chief cyber security adviser at Microsoft, told BBC News that the spike in spam is the result of higher capacity broadband, better operating systems, and higher power computers that allow criminals to easily send out billions of spam messages.

Increasingly, the report found, hackers are employing common file formats—Microsoft Office documents and Adobe's PDF format—to deliver malicious programs. Attacks using PDF files increased sharply in the second half of 2008, Microsoft noted.

According to the BBC, however, the PDF vulnerabilities exploited by criminals have been fixed by Adobe and do not exist in the latest versions. But more than 91% of attacks exploiting vulnerabilities in Microsoft Office took advantage of security holes that had been plugged by updates available for more than two years. ■

Email Management: The Good, the Bad, and the Ugly

Doug Miles, Infonomics, July.August.09, Volume 23, Number 4, www.infonomicsmag.com

Like it or not, email is the nerve system of modern business. Compared to the phone, it is asynchronous and provides a written record to the sender and recipient for follow-up action or later reference. In this respect, it is much more useful than instant messaging or social networks.

It can be frivolous or deadly serious—it's possible to be fired via an email, but also due to an email. Many vital decisions are made by email exchange, and the implication of our usage findings is that these may be made on the move, on tiny screens, and when otherwise off-duty.

Whether within their own office or between organizations separated by thousands of miles and many time zones, the sender will assume that all sent emails are received, and that they are read.

They will frequently expect a response within hours, let alone days. All this despite the ease of misaddressing, the hit-or-miss nature of mobile synchronization, the spam filters, the reply-to-all clutter, and the mass deletions required to stand any chance of keeping one's inbox usable.

A mere four years ago, one of the questions in the AIIM email survey was "Which of your business interactions are likely to be carried out via email?" Today, email is pervasive across all aspects of all businesses—and it is highly business-critical.

For many information workers, the email client is their primary business application. They spend many hours of the office day reading, responding and collaborating via emails. Indeed, this survey shows that most also spend considerable amounts of out-of-office time checking emails and "staying in touch" with work.

Strange, then, that the email history created by these responses and interactions is so poorly maintained, and the ability of knowledge workers to search for important content within current and past emails—their own and those of their colleagues—is so poor.

In a large organization, several millions of emails are handled each day. Most are of no lasting consequence, but each day there will be a significant number of important emails involving the organization in obligations, agreements, contracts, regulations and discussions, all of which might be of legal significance.

In this report we discuss how these important records are being dealt with, what policies are in place, how aware staff are of the issues, and which technologies are in use.

For the discussions within this report, an email management system may be a specialized stand-alone system or an integration of an enterprise content management (ECM) or records management system with the email client.

KEY FINDINGS

- On average, our respondents spend more than an hour and a half per day processing their emails, with one in five spending three or more hours of their day.
- Over half have hand-held access by phones, Blackberries and PDAs. Two thirds process work-related emails outside office hours with 28 percent confessing to doing so "after work, on weekends and during vacations."
- "Sheer overload" is reported as the biggest problem with email as a business tool, followed closely by "Finding and recovering past emails" and "Keeping track of actions."
- Email archiving, legal discovery, findability and storage volumes are the biggest current concerns within organizations, with security and spam now considered less of a concern by respondents.

See Email Management on page 6

Email Management, continued from page 5

- Over half of respondents are "not confident" or only "slightly confident" that emails related to documenting commitments and obligations made by staff are recorded, complete and retrievable.
- Only 10 percent of organizations have completed an enterprise-wide email management initiative, with 20 percent currently rolling out a project. Even in larger organizations, 17 percent have no plans, although the remaining 29 percent are planning to start sometime in the next two years.
- Some 45 percent of organizations (including the largest ones) do not have a policy on Outlook "Archive settings," so most users will likely create .pst archive files on local drives.
- Only 19 percent of those surveyed capture important emails to a dedicated email management system or to a general purpose ECM system; 18 percent print emails and file as paper, and a worrying 45 percent file in non-shared personal Outlook folders.
- A third of organizations have no policy to deal with legal discovery, 40 percent would likely have to search backup tapes, and 23 percent feel they would have gaps from deleted emails. Only 16 percent have retention policies that would justify deleted emails.
- Overall, respondents plan to spend more on email management software in 2009 than 2008.

CONCLUSION

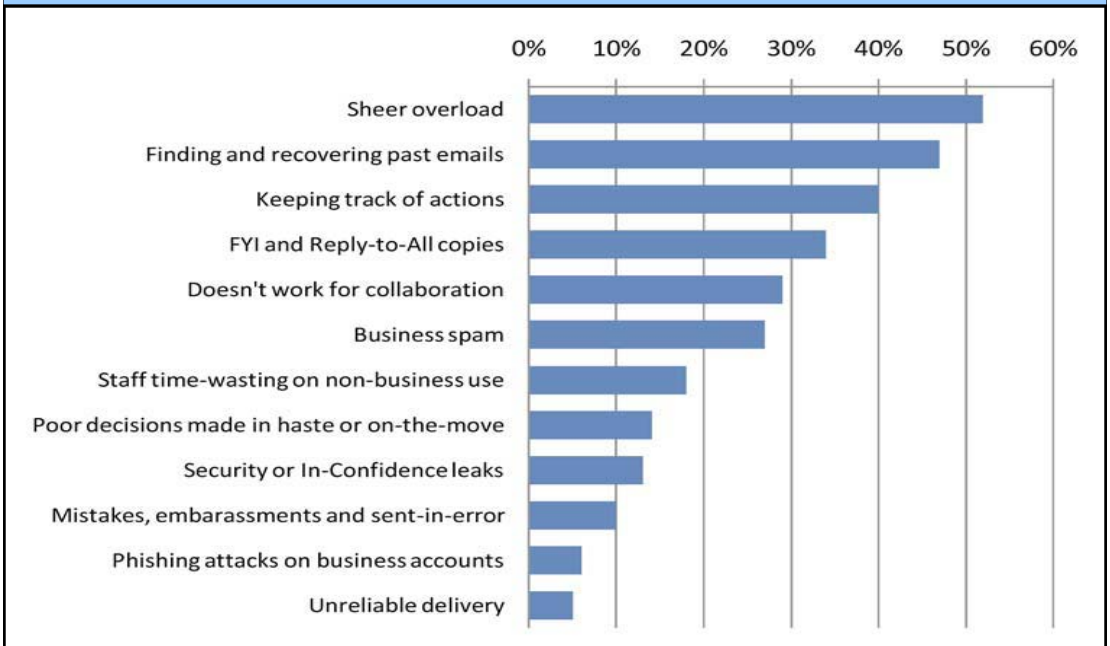
Taking the report's subtitle as a lead, the good news is that email management issues are now better understood, and a third of organizations plan fresh investment in this area over the next two years.

The bad news is that even within their current technology limits, over 50 percent of organizations have set no policies for dealing with important emails as shareable and retrievable records, nor do they have policies for legal discovery processes.

There are many ugly findings. Probably the worst is that most organizations are not protecting users from the misleadingly named "archive" setting within the Outlook mail client, which as a default moves older emails from the server onto the local hard drive.

Another ugly one is that 40 percent of organizations might need to search backup tapes in the event of a legal discovery requirement, and that 84 percent would have no way to justify why emails of a certain age or type had been deleted. ■

What poll respondents indicated as "The biggest problems generally with email as a business tool."



Clouds on the Information Horizon: How to Avoid the Storm

Brent Gatewood, CRM, Information Management Journal, July/August.09, www.arma.org

While much has been written about cloud computing, there has been little focus on the implications for applying records management rules to information stored in the clouds..Without that understanding, organizations cannot make informed decisions about using these resources. This understanding begins with a couple of definitions.

Generally, clouds are large collections of easily usable and accessible virtualized resources (i.e., hardware, development platforms, and/or services). These resources can be easily reconfigured to match varying service demands (loads) allowing the service provider to adjust for optimal resource utilization. A few examples include resources offered by Amazon, Google, and IBM.

There is an interdependence between cloud computing and software-as-a-service (SaaS). SaaS, which is commonly defined as a software delivery method that provides access to applications and functionality through remote access to a web-based service/ infrastructure, typically operates in the cloud. With SaaS, applications are not owned by the user; access and use are licensed for a defined period of time from an application service provider. This can save the licensing organization money for software, hardware, support, and maintenance.

This article relates to records and information being stored in a SaaS/cloud environment—whether created in an organization's captive environment or outside of its in-house computing systems. Information in the cloud resides in server farms and data warehousing facilities that may be spread throughout the country or even globally. Even though an organization may be doing business with a vendor down the street, its data may be stored many states away—or even in a different country.

As vendors identify needs and applications in the market and rush to develop and present cloud-based solutions, their ideas may not be fully developed or include records management rules-based control.

Not knowing where their information is stored and not having records management control over it are two major compliance concerns for organizations storing their records in the cloud environment.

TYPICAL CLOUD MATTER

The number and variety of cloud-based applications is growing rapidly, and many organizations either already use a SaaS solution or are considering one. Following are some of the most common types of solutions.

Communications

Communications are a natural fit for cloud computing solutions because they almost uniformly rely on the same basic infrastructure—the Internet. Email and instant messaging rely on the Internet for their delivery—and as such, it makes sense that email was one of the first solutions to be offered in the cloud.

Email and instant messaging rely on the Internet for their delivery—and as such, it makes sense that email was one of the first solutions to be offered in the cloud.

Having communications hosted by a SaaS provider has many benefits to an organization, especially because email is one of the largest consumers of technology resources in most organizations. Outsourcing some or all email infrastructure can free IT/IS resources for tasks more central to the organization's business. However, due to email's pervasiveness, many of an organization's records and a substantial amount of risk reside in email; managing these records and associated risks in the cloud can be problematic.

See Cloud on page 8

Cloud, continued from page 7

Document Management

Many organizations are also experimenting with some form of document management in the cloud. These applications range from ad hoc repositories for external access to very specific point solutions for defined departments and document sets. Typically, the level of control surrounding the application and content rises as the solution becomes more narrow and specific to a task or function. More generalized implementations typically have fewer controls compared to highly specialized point solutions.

Structured Data Service

Some structured data services have also been very prominent in the SaaS environment. Customer relationship management solutions have been successfully moved to the cloud. There has also been some success in moving enterprise resource planning toward cloud-based applications. These examples rely on a structured data set and capture methodologies, as well as an enterprise need for the information they contain. This broad need and tightly managed capture methodology and controlled data set work well in the structured environment. The caution arises because, in some cases, the complexity of the information captured may require more stringent management controls.

Business Continuity

Another good application for cloud computing is disaster recovery and business continuity. Utilizing the cloud infrastructure for storing or managing business-critical information makes sense if the proper controls are in place. Running parallel systems offering failover capabilities (the ability to automatically switch to a redundant system in case of system failure) makes sense for many business-critical systems. Of course, running duplicate systems can be costly, so the value of the potential reduction in risk for a critical system must be measured carefully to ensure the investment is worthwhile.

STORM CLOUDS ON THE HORIZON

Cloud computing has a definite place in today's organizations and is likely to become even more prevalent. However, records management compliance ramifications of SaaS solutions must be fully considered before they are implemented. Although the cloud has its advantages, it also has disadvantages. An organization's RIM, IT, and legal staff must understand those disadvantages in order to identify possible problems and minimize risks of any SaaS solution that is being considered or has already been implemented. Primarily, they must understand the legal and regulatory environment and risks associated with cloud use.

To say the legal environment is changing would be an understatement. The current economic situation and its causes ensure that regulatory oversight around the world will grow in the coming years. But current requirements associated with how an organization handles its information are already very demanding. Following is an examination of some of the more prominent issues surrounding records management and how they are affected by cloud computing.

FRCP Related to Discovery

The most recent update to the *U.S. Federal Rules of Civil Procedure*, which occurred in December 2006, places a large burden on an organization preparing for discovery.

Rule 26(a)(1)(A)(ii) states that, in a lawsuit, an organization must provide to its opponent a copy—or a description by category and location—of all documents, electronically stored information, and tangible things the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment.

The current economic situation and its causes ensure that regulatory oversight around the world will grow in the coming years.

Rule 26(a)(1)(C) states the time for initial disclosures—in general. A party must make the initial disclosures at or within 14 days after the parties' Rule 26(f) conference unless a different time is set by stipulation or court order, or unless a party objects during the conference that initial disclosures are not appropriate in this action and states the objection in the proposed discovery plan. In ruling on the objection, the court must determine what disclosures, if any, are to be made and must set the time for disclosure.

See Cloud on page 9

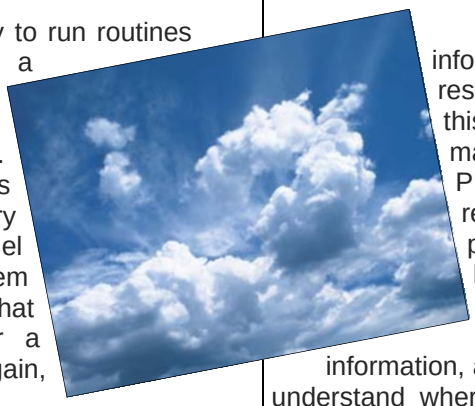
Cloud, continued from page 8

Consider what these statements mean to organizations preparing for a pre-trial meeting. Putting together a listing and map of all relevant and responsive data within an organization within the 14-day time frame will be difficult enough. Add to that the difficulty of identifying and documenting vendor relationships and data stored with multiple vendors in the cloud. It is unacceptable to say, "The information is out there, someplace." Organizations must identify the location of relevant information and verify the information has not been and cannot be altered. How is this done in the cloud?

Regulatory Requirements

Regulatory agencies also require information be accessible for review and audit purposes. If the information has been used to report compliance activities, it is critical to show the requesting agency the information remains unaltered from its previous state.

It may also be necessary to run routines and produce reports in a manner similar (or exactly) as they were run for the original reporting purposes. With in-house systems, it is fairly easy to show regulatory agencies and audit personnel the current state of a system and the upgrades, if any, that have been performed over a specific period of time. Again, how is this done in the cloud?



Privacy Concerns

Privacy is one of the longest standing and most important concerns with cloud computing. Consider the lengths organizations must go to ensure information repositories are secure in their own controlled environments. Now, consider the difficulty of that task in a typical cloud environment, remembering that a large-scale solution with multiple clients and shared architecture is what makes cloud computing powerful and economical. In fact, a SaaS provider may be relying on other external providers for its backbone, infrastructure, and storage.

An organization's information may be resident in several locations and may coexist with other clients' data. Depending on the type of data or the location of the data, this may result in a host of legal issues and legal violations. At the very least, an organization's clients—internal and external—may have a strong, negative reaction to learning their information is not being held internally by the organization. Everyone, from management to individuals, wants to know their private information is secure. How is this done in the cloud?

One of the reasons that SaaS and cloud computing are appealing is the solution can be globally deployed much easier than if the organization had to push hardware and software out to each and every location around the world. The allure of an easy and cost-efficient global deployment may mean a shorter review and development cycle—and less initial attention to privacy and compliance issues. This shorter cycle is often where transborder issues are missed. However, if an organization does business internationally, it has no choice but to consider the international data management and compliance obligations and restrictions that are implicated by a cloud computing model.

Personally identifiable information (PII) is subject to many restrictions worldwide. Transferring this information to a SaaS provider may violate some countries' laws. PII is not the only issue. Country restrictions vary, but information potentially subject to privacy, location, and other restrictions can include financial data, intellectual property, health information, and much more. It is imperative to understand where this data resides and how to restrict its movement and access to it as necessary. With cloud computing, this may not be possible.

The combination of a widely deployed infrastructure in multiple locations makes managing these issues problematic. If a SaaS provider is utilizing a second or even third tier of vendors to help manage its systems, as is often the case, the problem is aggravated—not only does an organization not know what is being done with its data, it may not even know who the other providers are. Cloud computing models can ignore these problems and make compliance and verification of compliance difficult, if not impossible.

See Cloud on page 9

Cloud, continued from page 8

Coming Regulations

Looking forward, new regulations and case law that will affect how records are kept and managed are on the horizon in the United States and abroad. The current U.S. administration has mandated transparency and accountability. These tenets will be the cornerstones of new regulations that will soon be in force. Transparency and accountability will drive future records management directives much like the Sarbanes-Oxley Act of 2002 did before them. It is critical that any solution, inside the organization or outside, be prepared for this new mandate as it relates to records and information.

This means, while organizations must maintain easy access to information, having appropriate management controls will be even more important tomorrow than it is today. Where information is maintained, how it is managed, and how the information is used to support an organization will drive the development of new compliance strategies and tools. "How is this done in the cloud?" is a question that organizations must answer specific to its records requirements.

While organizations must maintain easy access to information, having appropriate management controls will be even more important tomorrow than it is today.

COMPLIANCE IN THE CLOUD?

Records management compliance is difficult enough inside of an organization, even when it is using its own best practices tool set. Is it possible for an organization that is storing information in the cloud to be compliant with the many rules and regulations specific to it and its information? The answer is likely, "No."

Yes, it is possible to define rules to manage aspects of the life cycle and disposition of the information that is resident in the cloud. But these rules are difficult to enforce, unlike a consolidated rule set managing information resident within an organization's internal environment.

Proper records management requires a centralized control point, as well as effective enforcement for an organization's records management tool set to be effective. Today, the controls in place with most SaaS providers are too non-specific. The controls in place are collection-focused and largely managed according to the provider's rules, not those of the organization whose information is being stored.

To truly satisfy the records management needs of most organizations, control and management of data in the cloud would need to reside inside of the organization itself and extend to cloud-based repositories. A centralized tool managing life cycle rules for the organization would need to have the proper hooks into the data resident in the cloud. True federation of records management controls will need to expand beyond the organization itself and into the data repositories outside of the organization. These tools need to have a complete view of the information owned by the organization to be responsive to internal and external requests. These tools do not exist today.

STEPS TOWARD COMPLIANCE

The reality is this: The tools may not exist, but organizations are moving—or have already moved—data into the cloud. Now what?

Data relationships and management controls inside of organizations are more important than ever. Unless the management controls are already in place, it is unlikely that individuals are going to seek advice about extending controls to cloud-based repositories.

Education and proactive relationships driven by a strong records management function will help identify cloud-based initiatives early and raise awareness throughout the organization. Once it has been identified, an organization can look at an initiative's scope and explore deployment of reasonable controls that it can put in place. See the next page for "Checklist for Evaluating Cloud-Based Initiatives" which includes questions about issues an organization must answer when considering a cloud-based solution.

Cloud computing is not going away. It can be a valuable tool that needs to be understood and managed. Records management, with the proper relationships in legal and information technology and services, can help to reasonably manage information in the cloud. ■

CHECKLIST FOR EVALUATING CLOUD-BASED INITIATIVES

Organizations considering a cloud-based initiative—or reviewing a solution already in place—must explore the answers to the questions about the following issues:

CONTRACTS

- What service are we contracting for and what are the vendor's records management and compliance obligations?
- What kind of controls does the vendor have in place?
- How is information destroyed?
- Can we set minimum and maximum retentions and at what level?
- Are there secure destruction options?
- What are the vendor's policies for backups, replication, or failover?
- How do we confirm disposition takes place on a timely basis and according to our rules?

AUDIT CONTROLS

- What is the provider's internal audit process?
- How often is the provider audited by external agencies?
- To what standards is the provider held?
- Is the vendor open to being audited for compliance? (If not, this may be a sign of bigger issues.)

INTEGRATION POINTS

- Is the vendor open to integration with our systems and applications?
- Has the vendor integrated with any systems that provide a structure for compliance?

POLICIES AND PROCEDURES

- Are the vendor's policies and procedures related to handling and managing our information acceptable?

  If they are not, either move or don't store the data or have the vendor make an auditable change specific to the needs of your data and organization.

FOLLOW THE DATA

- Can the vendor provide a data map detailing where the information resides?

  A data map is **mandatory**. As necessary, ask for help in reviewing this information since it will likely be complicated as it details infrastructure and possible third-party relationships specific to your data. You need to understand the implications of this scheme to your organization.

Why Your Email Inbox is Not a Good To-Do List

Source: Leo Babauta, http://zenhabits.net

New York Times technology writer David Pogue, a writer I admire, recently listed some of his best productivity tips — and it's a good list. One thing I noted with interest is that he uses his email inbox as a to-do list, which is a fairly common practice.

And while there's certainly nothing wrong with that, and I've done it myself, I wanted to make a quick counterargument.

An email inbox isn't the best to-do list, and here's why:

1. **You can't change the subject lines**. This means your to-do list is made up of subject lines that often have nothing to do with the action you need to take. An email that says "today's meeting" might really be an action to call someone or send a file to someone. You'll need to open each email to find the actions, which is very inefficient. Or, you'll need to remember what actions are associated with each email, and that defeats the point of a to-do list … the list is supposed to remember for you, and take the stress away from your brain.

2. **There might be multiple actions in each email**. What if an email contains 10 to-do items? You can't delete or archive the email when you've done one or two of the actions. It'll remain in your inbox until all 10 are done, as if nothing has been done. Also, you might forget that there are multiple actions in an email and file or delete it when you've done one of the actions—either that or you'll be forced to remember that there are multiple actions in the email, again defeating the purpose of a to-do list.

3. **You can't re-order the emails (usually)**. Many email programs (such as the wonderful Gmail) just show the emails in the order they come in. Which means if you want to put the most important items at the top, you can't. If you want to group all the items for errands, you'll have to create a label for that and look there. It's not as flexible as even the most simple to-do program.

4. **You can't prioritize your to-dos**. Most readers know that I'm a fan of choosing your top 3 Most Important Tasks each day (see The Power of Less and Zen To Done for more). But you can't list just your top 3 Most Important Tasks in email—you have to list them all. In the order they come in. It's possible to do a workaround for this, and create a label or folder just for important tasks, but then why use your email as a to-do list? Why not use an actual to-do list that works the way it's supposed to?

5. **An email inbox contains distractions**. This is probably the worst thing on this list: if you're looking at your to-do's in email, you're in very big danger of new emails coming in and distracting you. I think it's a bad idea to have email on all the time—it makes it difficult to focus. I'd prefer a simple to-do list that allows you to shut off email while you're trying to get important work done.

So what's a better method? Simple: choose a simple to-do list and as you process your email inbox, pull out the actions to the to-do list. A notebook or index card works fine, as does a simple program such as Taskpaper (my current favorite) or even a text file in Notepad or TextEdit. If you set up a keyboard shortcut for your to-do app or file, it just takes a second to copy and paste a to-do from an email.

I'm not saying you can't work well and get great things done using an email inbox as a to-do list. David Pogue obviously manages to get a lot done this way, and I've done it from time to time. But it's not the best way, at least for those who like a simple way to find individual, actionable items, to prioritize tasks, and to work without distractions. ■

RECORDS AND INFORMATION MANAGEMENT RESOURCES

AIIM-The Enterprise Content Management Association—AIIM is the international authority on Enterprise Content Management (ECM) - the tools and technologies used to capture, manage, store, preserve, and deliver content and documents related to organizational processes. ECM enables four key business drivers: Continuity, Collaboration, Compliance, and Costs. www.aiim.org.

ARMA International—is a not-for-profit professional association and the authority on managing records and information – paper and electronic. www.arma.org.

Bitpipe.com—is the definitive guide to online resources for IT professionals. Provides information through technology white papers, webcasts, case studies and IT product information. www.bitpipe.com

British Columbia Corporate Information Management Branch—CIMB provides central information management services and support to ministries, Crown corporations and agencies within the Government of British Columbia. CIMB is responsible for government recorded information management policy, standards and procedures. www.cio.gov.bc.ca/services/records/

Civic Info BC—Civic Info BC is a cooperative information service for those who work or have an interest in BC's local government sector. www.civicinfo.bc.ca

Gartner—global leader in technology-related research and advice. www.gartner.com

Forrester Research—Forrester Research, Inc. is an independent technology and market research company providing advice to global leaders in business and technology. www.forrester.com

IDC—International Data Corporation—get the latest trends, surveys and forecasts. www.idc.com

ISO—International Organization for Standardization—check out the latest information on ISO 15489, the world's first standard for records management. www.iso.org.

Library and Archives Canada—Library and Archives Canada collects and preserves Canada's documentary heritage, and makes it accessible to all Canadians. This heritage includes publications, archival records, sound and audio-visual materials, photographs, artworks, and electronic documents such as websites. As part of Library and Archives Canada's mandate, they work closely with other archives and libraries to acquire and share these materials as widely as possible. www.collectionscanada.ca

Local Government Management Association of BC (LGMA)—LGMA is a professional organization representing municipal and regional district managers, administrators, clerks, treasurers and other local government officials in BC. www.lgma.ca

National Archives and Records Administration (USA) (NARA)—Of all documents and materials created in the course of business conducted by the United States Federal government, only 1%-3% are so important for legal or historical reasons. These documents are kept by NARA forever. Learn about NARA's record keeping standards. www.archives.gov.

SearchCIO.com—is part of the TechTarget network of industry-specific IT Web Sites. Get the latest news on everything that matters to CIO's! http://searchcio.techtarget.com.

UPCOMING TRAINING OPPORTUNITIES in Victoria, BC

Introduction to Records & Information Management
A one-day workshop covering the basics of records and information management.
October 7, 2009

Using ARCS, ORCS and LGMA
A one-day workshop teaching the basic skills needed to master functional-subject based classification systems like ARCS, ORCS, or LGMA.
October 14, 2009

Effective E-Mail Management
A one-day workshop for Executives and others who want to get a handle on their e-mail.
October 21, 2009

Designing Records Classification Systems
A two-day workshop providing practical hands-on experience in developing file taxonomies.
November 9-10, 2009

Planning & Implementing Your RIM Program
A two-day workshop providing the tools and skills needed for developing a RIM program.
November 16-17, 2009

Preparing Records for Offsite Storage
A one-day workshop providing practical hands-on experience on how to prepare records for offsite storage.
May 6, 2010

For more information and to register, go to:
www.rimsolutions.ca or
www.24carrotlearning.com

Prefer to speak to someone instead?
250-658-4873