A STRATEGY PAPER FROM CENTER FOR DIGITAL GOVERNMENT

HIT ANY KEY…
Except Send or Delete

E-mail Security and Availability in the Age of Digital Records

"[E-mail is] proof that a million monkeys typing randomly at keyboards would NOT produce a Shakespeare play."
— Commendatore, August 12, 2003

Introduction

Fully three-quarters of mission critical data is contained in, or transported by, e-mail within large organizations.[1] Moreover, as a greater percentage of the total government record store becomes digital, the ease with which data can be legitimately shared or illegitimately misused or stolen increases exponentially. By extension, protecting e-mail from external and internal threats, keeping it secure, and ensuring availability are now mission critical objectives. Government organizations face additional challenges managing e-mail in a manner consistent with their respective public records laws. Also, they operate within an increasingly complex regulatory compliance layer of additional federal mandates. Within this context it is somewhat understandable why some governments have yet to come to grips with the challenge. Yet there are public sector organizations making progress through improved e-mail management policies, processes and products. Nevertheless, governments must first overcome a number of key barriers to successfully manage e-mail.

Obstacle 1: Lost in the Maze

NAVIGATING THE REGULATORY AND COMPLIANCE ENVIRONMENT

Like a high performance horse in a steeplechase, government also has obstacles to overcome in order to reach the finish line without a catastrophic fall. Governments' aging public records laws — many of them written over twenty years ago — stand as a set of major obstacles to be cleared. While there may be general agreement about the need to revise components of public records laws, there is also the fear that the cure will be worse than the disease.

Yet there is reason for optimism. There is a great deal of interest in how the information assets of government are treated, as evidenced by near daily press accounts on the subject. It is also an item on federal and state legislative agendas each year and under constant scrutiny in Congress. The Center for Public Integrity[2] estimates that public disclosure[3] laws — the cornerstone of open government — have been eclipsed more than 300 times by amendments in the last four years, all in the name of national security.[4] Scandals, pressure on the sound governance of business government, not to mention heightened security, security breaches and the flood of spam and other malware are converging trends. These trends have created a "perfect storm" that makes it more difficult for state and local governments to ignore records management issues. On the face of it, there is an urgent need for better planned, orderly and more reliable solutions to the e-mail management dilemma.

Perhaps the only thing that matches the urgency of the need for e-mail management is the complexity of navigating the law, policy and practice processes that must be used to create change. It is difficult to draw general conclusions about the effects of public records laws on state and local government because, like each individual public records law, the ways that governments manage their information are diverse and unpredictable, rather than homogeneous. Furthermore, the great range of data volumes and information technology (IT) infrastructure complexities exacerbate the problem of trying to develop a general picture.

Indeed, states vary widely in the ways they treat the unique balance between the individual right to privacy and the public's right to know and access information about government activities based on their respective histories and priorities. For example, states have reached no universal conclusion about how to treat e-mail. However, the majority of states do not define e-mail as a public record.

Instead, many support the originating agency's right to determine which e-mails are public records, based upon content. Other states have decided that e-mail *is* a public record (Colorado and Rhode Island), but some restrictions apply to personally identifiable information provided by citizens to the government to protect that information from disclosure. The National Conference of State Legislatures (NCSL) has a review of state laws governing e-mail.[5] Also, federal laws or regulations, the Health Insurance Portability and Accountability Act (HIPAA) being a prime example, add an additional layer of complexity to existing public records laws. To top off the confusion, state and local governments are involved in a myriad of internal investigatory actions while others are engaged in litigation that requires electronic records production, especially e-mail.

Regulations from the IRS and other entities within the Department of Justice, such as the FBI, may also affect what kind of information is transmitted over e-mail communications, how it is transmitted (some require encryption) and what happens with the information once it is received (records retention).

An already complex and ambitious environment is further confounded by the Sarbanes-Oxley (SOX) wildcard – that is, the potential

HOW DO YOU SPELL COMPLIANCE? *HIPAA* AND *SOX*

About HIPAA and Sarbanes-Oxley

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a law that was enacted by Congress in 1996. Relevant to e-mail management are the Title II provisions that establish national standards for security, privacy and electronic data interchange of health data. Multiple organizations within state and local government are covered under the umbrella of HIPAA, and therefore must comply with the law and with the U.S. Department of Health and Human Services regulations that interpret the law.[6,7]

Sarbanes-Oxley (SOX)

In the wake of Enron and other corporate scandals, the Sarbanes-Oxley Act (SOX) was established by the U.S. Congress in 2002 with far reaching effects, ranging from the freezing and dissolution of future company pensions to the restructuring of corporate America's oversight boards. While SOX only applies to publicly held companies, it serves as a fair example of the need for good governance.

The American Society of Association Executives summarizes thirteen key provisions of SOX.[8] The SOX provisions most likely to have an impact on government are the audit, document destruction or alteration, and internal control provisions. The federal government is already establishing new internal controls via SOX-like provisions. The internal controls framework is published by the Committee of Sponsoring Organizations (COSO)[9], an umbrella group of accounting and financial management organizations. The framework forms the backbone of Sarbanes-Oxley's section 404. The Government Accountability Office (GAO), the investigative arm of Congress, has adopted the COSO framework for the federal government. It should be noted that although state and local government do not currently fall under the umbrella mandate of SOX, voluntary compliance to some SOX provisions or even "copycat" legislation at the state level may be in the offing.[10]

SEC Storage of Electronic Records Rule 17-CFR 270.17a-4

Since 1934, the U.S. Securities and Exchange Commission (SEC) has had a comprehensive set of rules that govern the preservation of records. These rules have been updated to require brokers, dealers and exchange members to follow electronic storage management procedures including e-mail management. Although these requirements, not unlike SOX, only apply to the securities industry, many of these practices provide excellent guidance for better management of electronic government records. Courts are increasingly relying upon e-mail to support the discovery process when suits involving a government are filed. Discovery is frequently a labor intensive process that can be aided significantly by modern searchable e-mail archiving and storage tools.

The issue is that e-mail and other electronic communications technology (including instant messaging, text-messaging, e-mail enabled phones and wireless-enabled handheld devices) are increasingly being used to execute and document major business transactions and policy decisions, yet are not retained in a disciplined way for future inspection or disclosure — violating the spirit of SOX and the letter of state public disclosure laws.

residual affect of Sarbanes-Oxley on state and local government's information practices (see the "How Do You Spell Compliance?" sidebar).

The extent to which scandals in the public and private sector will usher in a new wave of governmental accountability at the state and local level remains to be seen, but interest in the collection and management of government information is very high on many groups' public agendas. Additionally, SOX contains a number of useful best practices that governments should consider adopting.[11] Therefore, governments serious about developing and implementing a comprehensive e-mail management plan should look carefully at models developed as part of SOX compliance — particularly as they relate to policies for audit, internal control and records retention.

Obstacle 2: Cyber-Threats

Cyber-threats are increasing in volume, complexity and virulence. Threats are becoming more targeted and are more focused on financial gain. Industry experts are observing how cyber-criminals work together to pool their talents. Spam is being used as a way to disperse phishing e-mail.[13] The volume of e-mail sent to organizations will grow by 25 to 30 percent annually through 2009, with more than 60 percent of e-mails sent being spam.[14] Adding to the burgeoning problems of spam are other threats known by an encyclopedic list of names such as phishing, pharming, spyware, zombies, viruses, keyloggers, Trojan horses and other forms of malware, which most often find their way onto a network via e-mail.[15] For example, data shows that over 90 percent of viruses enter networks through the e-mail gateway.[16] Such threats can result in vast and increasing volumes of e-mail that must be managed. In addition, governments also experience identity and other forms of data theft, destruction or alteration as a direct or indirect result of e-mail security vulnerabilities.

E-MAIL – A MATTER OF PUBLIC TRUST

In August 2005, the United States government issued subpoenas to Google, Yahoo, Microsoft and AOL to turn over search information about millions of users. While the other named companies have since complied with their subpoenas, the Department of Justice said that Google repeatedly refused these demands. Meanwhile, as the government continued to press claims in the courts, the reaction from civil libertarians was swift. "You have to be alarmed at the idea that the government can come in and say, 'I want you to give me your statistical data.' This could be the first step on the way for asking for the content of the e-mails," said Shayana Kadidal, an attorney for the Center for Constitutional Rights.[12]

At this point, the government has not actually requested user information that personally identifies individuals, their names or computer internet protocol (IP) addresses. Nonetheless, privacy advocates fear that the government, using sophisticated data mining techniques, may recognize patterns in the user data that create a trail of bread crumbs created by the search requests and its results, leading to possible suspects, potential future subpoenas and further investigations. While privacy advocates worry that the government will subvert freedom in a fruitless search to save it, advocates for public safety and criminal justice claim that only law breakers have a reason to fear public disclosure of their activities and words.

Yet in this highly visible and increasingly polarized public debate, there are some common threads that tie together otherwise separate discussions about the war on terror, Internet pornography, search engine technology companies and e-mail management. Each arena must confront the fundamental role of government and its relationships to the broad reaching issues of privacy and security in an Internet-aware, post Sept.11 world. How e-mail is and will be managed for the foreseeable future is being directly affected by these large canvass issues that drive the public mood — and the tenor and substance of the public policy debate in state houses and in Congress. Consequently, public officials must keep these contextual issues constantly in their peripheral vision. Failure to do so brings with it the risk of losing sight of them and subsequently being surprised by them when they re-appear.

The operational and policy aspects of effectively managing e-mail are markedly different in scope from the broader discussions about "freedom vs. safety" that form the backdrop for debate. It is, however, the responsibility of the branches of government to decide together how best to manage records on behalf of citizens. Unfortunately, the past has yielded many stalemates that the future will be less inclined to permit. Some would argue that a government that cannot or will not effectively protect its records is a government not worth trusting. Such are the high stakes and risks associated with potential missteps in the management of digital records — and the 800-pound gorilla dwarfing the landscape of electronic records management is e-mail.

"Whenever a conflict arises between privacy and accountability, people demand the former for themselves and the latter for everybody else."
— David Brin, *The Transparent Society*

Many states are adopting specific laws to deal with spam as alternative ways to address these cyber-threats. According to the National Conference of State Legislatures (NCSL), 28 states considered statutes to combat spam, phishing and spyware in 2005. To date, new cybersecurity legislation has been adopted in 11 states.[17] Although some legal fixes may help in the long run, governments can achieve a more immediate impact by beefing up e-mail security as part of an overall e-mail management plan.

Obstacle 3: Policies and Infrastructure

Fortunately for government, there is a convergence of governments' need to address e-mail management problems and the solutions and tools needed to address them.

One of the long understood advantages of using IT to automate government processes is the need to make policies specific enough to be replicated by software or, more properly, codified in software. The effective use of automated tools for e-mail management relies on comprehensive e-mail management policies driven by a sound legal framework that addresses the protection of content and workflow of e-mail across its lifecycle. To that end, this paper now turns its attention to a five point plan for developing such a policy and practice framework.

FIVE THINGS STATE AND LOCAL GOVERNMENTS CAN DO TO HARNESS UNRULY E-MAIL

The following section will put forth five methods for help in regulating and managing e-mail. The points to follow will explain:

1. How and why to establish an e-mail management steering committee;
2. The purpose of an e-mail working group;
3. Points to include in an e-mail management and implementation plan;
4. Why to implement a formal project management process; and
5. How to implement the e-mail management project.

1. Establish an executive level e-mail enterprise policy and governance steering committee. The role of this governance committee will be to review and sign off on all plans, policies and implementation strategies of working groups that it establishes. This executive steering committee should be chartered by the chief executive officer (governor, mayor, city manager, county executive).

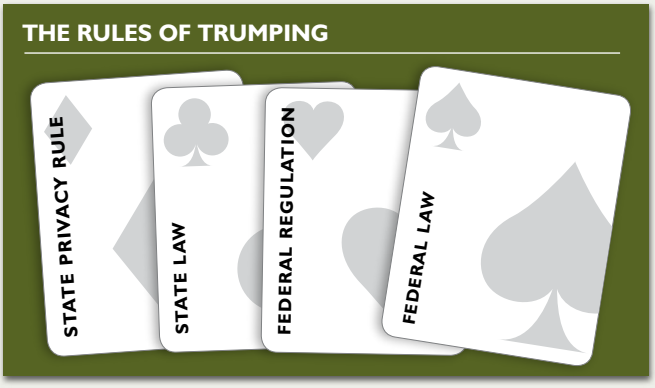
An already existing umbrella group that handles multiple IT issues could be tasked with developing and adopting a framework, including e-mail management. Alternatively, this could be an ad hoc group established specifically for an e-mail project. The committee should be composed of key stakeholders representing the program and IT side of the organization, and should cut across the enterprise.

For this group to function properly, the members need to either have policy making authority or a clear delegation of that authority from their executive. Possible members of the executive group might include the chief information officer (CIO), the chief information security officer (CISO), the chief privacy officer (CPO), major department executive directors or deputy directors, and staff to the committee.

One of the first responsibilities of the steering committee will be to charter the effort by articulating a common commitment to proper e-mail management. The steering committee should create and authorize the needed working groups and establish their scope, direction and timelines.

While smaller entities may not have these "C" level positions, it is important that the issues of security and privacy be part of at least one of the leader's portfolio so committee members receive proper emphasis in the discussions and decisions that this committee makes.

2. Establish an e-mail working group. This group is composed of both program and technical members. One early task of the working group would be to inventory all relevant laws (federal, state and local), rules, regulations and policies that apply to the public entity and any subunits of the organization. To decide where the "circles" or "fences" should be drawn, the group first needs to identify which data is relevant to these policies and at the same time must discover where that data resides. Particular attention should be paid to the complex web of statutory privacy and confidentiality provisions and retention schedules. Therefore, the working group should clearly understand what policies (statutes, rules and regulations) "trump" others.



3. Write an e-mail management strategy and implementation plan. The plan should describe the governance and other processes needed to improve the management of e-mail. The CISO and CPO or their designees (provided they have the delegated authority to act on their principals) should be involved in the drafting or oversight of the creation of the plan. The plan should also receive extensive input from the state or local government's IT architect. The IT architect will help the working group understand how best to integrate this project and future toolsets into the overall IT architecture and infrastructure. A prime example is to review the organization's current wireless footprint and determine if security measures are sufficiently robust to permit the transmission of wireless e-mail that contains, for example, HIPAA-related content.

This plan should map out and describe the administrative and user policies that need to be created to effectively drive the new e-mail management infrastructure. The plan should also recommend a process for policy creation and enforcement. Once complete, the plan should be approved by the executive steering group.

Any e-mail management strategy should be implemented in the context of an overall electronic records management strategy. The Minnesota State Archives is an excellent reference point for a governmental organization seeking to improve its e-records management. It not only provides the legal framework but also a series of guides including: electronic records management strategies, long-term preservation, Web content management, metadata standards, file naming and formats, electronic document management, and e-mail management.[18,19]

4. Implement a formal project management process. There is an extensive and well-established body of professional knowledge in project management that leaders can refer to for guidance. The Project Management Institute (PMI) is a membership organization that focuses on improving the professionalism of IT project management.[20] Any internal or external IT organization that develops, deploys and maintains IT systems and services should be very familiar with this field before carrying out IT projects. A formal project management office (PMO) should be closely involved in this process. If this role has not been established by the public entity, it should consider putting it into place. Minimally, this effort will help professionalize the e-mail project, but can professionalize all future IT efforts.

5. Implement an e-mail management project. Consistent with project management best practices, what follows is an annotated checklist to help get e-mail management right:

- **Conduct a formal requirements analysis.**
  Look for common or core requirements across the enterprise, as well as requirements that are unique. Select shared solutions wherever possible.
- **Standardize on a common e-mail platform.**
  A common e-mail solution deployed across the entire public entity's infrastructure will improve IT efficiency by reducing the complexity inherent in the numerous compatibility, security and configuration issues that arise in a heterogeneous e-mail environment. It also means that the deployment of automated patch management, e-mail archiving, data vault or back-up and recovery software will be less complex tasks when used in concert with a common e-mail platform.
- **Provide external e-mail security.**
  Reduce e-mail volume at the perimeter through the use of an anti-spam router.
- **Provide internal e-mail security.**
  Use the following proven tools consistently and with discipline:
  - automated patch management and delivery system;
  - anti-spam/anti-virus software;
  - spyware removal software; and,
  - content filtering software to prevent network user access to undesirable high security risk sites.
- **Create an e-mail archive.**
  Deploy software that auto-indexes e-mails including all attachments so they are searchable by word and/or phrase, auto-compresses/auto-moves e-mail to "near-line" or secondary storage based on established policies that organizations can configure within the software. This implementation is more than simply backing up e-mail.
- **Establish data vaults.**
  Configure data vaults to integrate and automate records retention policies.
- **Establish rapid back-up and recovery processes.**
  Leverage best practices that have already been automated through regulatory compliance and electronic discovery software (making modifications to reflect unique local requirements as necessary).
- **Set up e-mail storage management procedures.**
  Automate data migration through tools that assist movement between platforms while retaining high availability of the primary e-mail platform. This also assists in disaster recovery and continuity of operations.

A basic e-mail management infrastructure coupled with the governance structures and policies to support it will better position governments to make e-mail more secure and available within the context of public records laws and policies.

"Anything specific I need to do or tweak?… Are you proud of me? Can I quit now? Can I go home?"
— Michael Brown, Post-Katrina e-mail disclosures, September 2005

ACTION PLANS: HOW ONE GOVERNMENT GOT STARTED WITH E-MAIL MANAGEMENT

Oceanside, California, was looking for a more efficient way to comply with public records requests. City CIO Michael Sherwood succinctly identified the fundamental weakness of the city's e-mail system. "The e-mail system was not designed to be a searchable archive," Sherwood said. "It was designed to be a communications platform."

After researching a variety of solutions, Sherwood concluded that he would recommend the acquisition of a new e-mail vault system that was configurable so records retentions policies could be integrated and automated. "Since people have become aware of [e-mail content], public records requests are increasing," reported Sherwood. "They know we have the capability. If I had to make an educated guess, I'd say I've seen an increase of 10 to 20 percent in public records requests for e-mail over the last three years. Before that, public records requests for e-mail were basically zero."

Traditionally, governments have resisted providing e-mail to citizens or constituent action groups, saying it's not technologically possible. Sherwood says this reason can no longer be sustained. "[Private citizens and the media] are going to want it, and you can't keep coming up with the excuse that it's not possible," the Oceanside CIO reminds us. Sherwood has found that the e-mail vault considerably reduces the amount of time the city spends trying to produce e-mail-based public records, "especially during election years."[21]

Conclusion

The final outcomes of a comprehensive and successful e-mail management program implementation are: lower program and IT risks, increased employee productivity, and effectively managed regulatory and compliance policies. These results can occur within the context of a sound and balanced government information practice environment. But in order to do so, governments need to understand how to build an effective e-mail management infrastructure to reduce the volume and storage costs while still protecting against threats. Governments must do this in a complex environment that requires effective compliance and risk management, while also improving citizens' access to public records.

In the advent of a cybersecurity threat, the volume of e-mail balloons. Government ought to be aware that there are products and tools that address threats and manage the e-mail lifecycle from the gateway to the vault, from creation to permanent retention or ultimate deletion of a record.

In the end, something as mundane sounding as e-mail management goes to the core of public trust. In modern government, e-mail has emerged as both the central nervous system for doing the public's business, and the institutional memory of the body politic.

ENDNOTES

[1] See AIIM - The ECM Association, The Role of ECM in Storage Decisions: The Why, What, and How of Storing Business Critical Information, January 9, 2006 (as reported in the trade press).

[2] The Center for Public Integrity (www.publicintegrity.org) is a nonprofit research and reporting organization that provides investigative journalism in the public interest.

[3] The terms *public disclosure* and *open records* are terms applicable to state and local government, where *FOIA* (the Freedom of Information Act) means roughly the same thing at the federal level.

[4] Charles Lewis, "A Culture of Secrecy: What has Happened to the Principle that American Democracy Should be Accessible and Transparent?" *The Center for Public Integrity*, February 8, 2005.

[5] Pam Greenberg, "The Public Life of E-Mail." National Conference of State Legislatures, September 2002. http://www.ncsl.org/programs/pubs/902email.htm

[6] Centers for Medicare and Medicaid Services, HIPAA Security Final Rule. http://www.cms.hhs.gov/Securit yStandard/02_Regulations.asp#TopOfPage

[7] Department of Health and Human Services Office for Civil Rights, HIPAA Privacy Rule Summary. http://www.hhs.gov/ocr/privacysummary.pdf

[8] Hugh K. Webster, "Association Governance in the Post-Enron Era." Association Law & Policy, American Society of Association Executives, December 2003. http://www.asaenet.org/Publications/EnewsletterAr ticleDetail.cfm?ItemNumber=10991

[9] The Committee of Sponsoring Organizations (COSO), "Enterprise Risk Management — Integrated Framework." September 2004.

[10] Hugh K. Webster, "Association Governance in the Post-Enron Era." Association Law & Policy, December 2003. http://www.asaenet.org/Publications/EnewsletterArticleDetail.cfm?ItemNumber=10991

[11] Dave Norwood and Jon Jensen, "Business Continuity/Disaster Recovery Roundtable — Availability and Security of Your Business Critical Applications." Business & Technology Roundtable, David Eccles School of Business, University of Utah, January 26, 2006.

[12] From Leslie Boyd's article "Little consensus on phone taps, Internet spying" from the *Citizen-Times.com*, January 30, 2006.

[13] "*Phishing* is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers." From ComputerWorld, http://www.computerworld.com/securitytopics/security/story/0,10801,89096,00.html.

[14] Gartner and Symantec's "Internet Security Threat Report," March 2005.

[15] For definitions of these and other types of vulnerabilities and exposures, see Webopedia at http://webopedia.com/.

[16] IDC Global Networks, untitled paper. http://www.idcglobal.net/IDCWeb/downloads/Glossary%20-%20Definitions_website.pdf

[17] National Conference of State Legislatures, "Unsolicited Commercial E-Mail Advertisements (Anti-Spam Legislation), 2005 Legislative Activity." Updated December 23, 2005. http://www.ncsl.org/programs/lis/legislation/spam05.htm

[18] Minnesota State Archives, "Electronic Records Management." March 2004, Version 4. http://www.mnhs.org/preserve/records/electronicrecords/erintro.html

[19] Minnesota State Archives, "E-mail Management." March 2004, Version 4. http://www.mnhs.org/preserve/records/electronicrecords/eremail.html

[20] The Project Management Institute. http://www.pmi.org/

[21] Shane Peterson, "Unintended Consequences." *Government Technology*, Oct 04, 2004.

100 Blue Ravine Road
Folsom, CA 95630
916.932.1300 phone
916.932.1470 fax

www.centerdigitalgov.com

Underwritten by:

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

CENTER FOR DIGITAL GOVERNMENT

Acknowledgments:
Paul W. Taylor, Ph.D., Chief Strategy Officer for the Center for Digital Government and the Center for Digital Education
Al Sherwood, Senior Fellow for the Center for Digital Government and former deputy CIO for the state of Utah

The Center for Digital Government, a division of e.Republic, Inc., is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.

The Center's special reports and papers provide two decades of experience and insight into the most important policy and management issues facing governments, and offer strategic approaches for planning and implementing technology, funding sources, and case studies from jurisdictions.