

# Simply Speaking: Managing Messaging as a Corporate Record

By Peter Mojica, Vice President, Product Management & Business Development, AXS-One Inc.

Every major corporation should be aware of the lingering smoking gun effect. *Miriam Webster* provides the following definition for “smoking gun”: noun—“something that serves as conclusive evidence or proof, especially of a crime.”

In business, that “something” is all too often an apparently innocent document. Years ago, that document was created on an old Remington typewriter, loaded with three layers of carbon paper, signed in triplicate and distributed by the corporate secretary at the company’s annual board meeting. A copy was kept in a specific filing cabinet. All corporate communication of this type was paper-based. If your organization was investigated or sued and records were subpoenaed or required, you were reasonably confident of what corporate records you had and where and how they were stored. Now fast forward to the 21st century...

Operating at Internet velocity with little or no controls is a recipe for disaster. We know that e-mail (and, increasingly, instant messaging [IM]) are now the primary means of business communication. Proof of that fact is that e-mail is the most widely used application in the world, more so than the Internet browser, which trails as a distant second (IDC, 2002).

So why is this a problem? The fundamental issue is that most organizations have implemented applications such as e-mail and IM without putting the necessary policies and procedures in place to manage the explosive risks associated with them. The explosion—some might say abuse—in digital communications has resulted in a critical share of real business information (over 80% according to Gartner) now sitting unmanaged within the storage subsystems. These subsystems can be comprised of hundreds, maybe thousands, of e-mail and other servers that are strategically deployed in your and others’ offices and primary and secondary data centers around the world.

Back to the days of Remington typewriters...every piece of communication was, by today’s standards, a manually intensive task: typed letters, faxes, regular mail. Today, thanks to e-mail attachments, “CC:” and “BCC:,” hitting the send button can potentially have dire consequences for your organization. Increasingly, the protection of your organization’s intellectual property (as well as the potential for multi-million dollar lawsuits) depends on how effectively you are able to implement and enforce corporate-wide records compliance management policies. Are you knowingly or uninten-



Peter Mojica

Peter Mojica is vice president of product management and business development for New Jersey-based AXS-One, a leading provider of records compliance management software. Mojica is a thought leader in the fields of records management, corporate compliance and risk

mitigation, and speaks at numerous industry events annually.

Mojica has more than 18 years of information technology experience, primarily in the financial industry. He brings a broad range of sales, technology marketing, and information technology management expertise to AXS-One.

tionally creating the “smoking gun” syndrome, or do you have the situation under control?

## Reduce the Liability

The “2004 Workplace E-mail and IM Survey” from American Management Association and The ePolicy Institute found that 21% of all employers have had employee e-mail subpoenaed by courts and regulators and that 13% of lawsuits are triggered by employee e-mail. Given that the same study found that 65% of companies lack e-mail retention policies, how should an organization begin to manage e-mail as a corporate record?

First, an organization should consider e-mail and IM as part of its asset data records retention program. It must be cost efficient, effective, flexible, scalable and it must include the recommended practices detailed in the chart on the following page.

## Business Questions for Your Business Assessment

How should your organization self-assess in order to determine the key areas that require immediate attention? Assess the development needs necessary to enhance your business policies that will be executed, maintained, measured, improved and ultimately enforced electronically.

Today self-assessed and business policies must be a priority business decision with executive sponsorship. Decisions taken during the assessment phase will guide subsequent actions executed within your records compliance management program.

**Assessing your corporate regulatory requirements should be highest priority.**

**“Most organizations have implemented e-mail and IM without the necessary policies and procedures to manage the explosive risks.”**

It must include...	...for this simple reason
<p><b>A single platform</b> for compliance, legal discovery and operational mail management capable of handling multiple e-mail platforms and more than just e-mail.</p>	<p>Managing and integrating multiple systems, even best of breed's silos, will increase the cost, complexity and overall systems maintenance. Higher-error rates are likely to occur.</p>
<p><b>A records management framework</b> for automated retention, disposition and legal case management. Comprehensive ability to develop global and explicit policies that conform to the business objectives.</p>	<p>Retention and disposition is core to the overall system. The retention capability must be flexible to codify business workflows and supply key principles such as process chain of custody for all records managed.</p>
<p><b>Irrefutable evidence capture</b>, blocking, supervision, fully customizable post-review. Real-time message capture, all inbound and outbound messages and transactions including various systems log files.</p>	<p>In-flight capture of electronic records is necessary in order to preserve authenticity and irrefutability of the data in the event of litigation.</p>
<p><b>Operational efficiency for storage</b> to simultaneously reduce storage burden across e-mail servers, consolidate server resources, increase storage utilization, reduce network back-ups.</p>	<p>Solve more business problems, within the same technological infrastructure, in a more immediate fashion by reducing the capital and operational expenditures associated with storage management.</p>
<p><b>Web services</b> interface for deep integration and application development. (i.e. pull archived message content seamlessly into other key systems).</p>	<p>The value of the archive is twofold: Managing risk and adding value through collaboration and integration of disparate data. Web services are the means to take advantage of the second.</p>
<p><b>Low Total Cost of Ownership (TCO)</b> for internal maintenance.</p>	<p>Recognize upfront that the enormity of the business problem is global and the consequences for long-term data storage, search and retrieval of it are of unprecedented proportions for the average business corporation.</p>

What does the law governing my particular business require relative to my corporation's information?

**Assessing the risk should come next.** Deciding on risk measurements will differ for every corporation. However, understanding the operations of divisional units first, then individual business cost centers contained within those divisions, can assist in determining core risk factors that make sense for your organization. The recommended areas of focus for most organizations come in the form of risk-to-profit, risk-to-reputation and risk-to-business disruption.

**Lastly, developing comprehensive policies that can be applied both globally and explicitly based on those risk fac-**

**tors should guide your choice of technologies to accomplish the given tasks.**

### Best Practice

From an IT perspective, the marching orders are clear: have a clear and comprehensive understanding of the business requirements and make "compliance" a key consideration for all IT projects moving forward. The immediate considerations should focus on four key areas; leadership; governance; technology; and competency.

**Leadership.** Senior management should drive compliance strategies; an organizational strategy must be defined first.

**Governance.** Roles, responsibilities and accountabilities must be clearly defined; a funding model must be established, organized to deliver.

**Technology.** A scalable infrastructure must be in place; standards and tools should be defined early on.

**Competency.** Recruiting and development of resources; a risk mitigation culture must be established.

By focusing on the immediate business problem first and ensuring that you can address broader requirements within the same platform later, your constituents will benefit from seamless compliance and assurance that a comprehensive and global approach to solving key business problems is well in hand. ■

***"Hitting the send button can potentially have dire consequences for your organization."***

AXS-One is a leading provider of records compliance management solutions. The AXS-One Compliance Platform enables organizations to implement secure, scalable and enforceable policies that address records management for corporate governance, legal discovery and industry regulations such as SEC17a-4, NASD 3010, Sarbanes-Oxley, HIPAA, the Patriot Act and Gramm-Leach-Bliley. AXS-One's technology has been critically acclaimed as best of class and delivers digital archiving, business process management, electronic document delivery and integrated records disposition and discovery for e-mail, instant messaging, images, SAP and other corporate records.