

Mitigating the Risks of Messaging

Recognizing and addressing the dangers of the casual nature of electronic messaging will minimize organizational risk. Putting an electronic communications plan in place is vital to protecting a company's reputation, its business interests, and its compliance success.

Maurene Caplan Grey

In any single day, millions of e-mail messages are sent and received by organizations – and nearly every day the media breaks the details about the latest scandal to be uncovered through evidence in those messages.

Protecting the organization by ensuring regulatory compliance is paramount in today's business environment, and many organizations start by securing e-mail. This is a necessary step – but a tactical one – that pursues only the “e-mail-as-evidence” pain point. Forward-thinking organizations are only at the cusp of realizing the magnitude of this quandary. The risks are not married solely to business regulations or to e-mail as a messaging medium.

Compliance

Stringent Securities and Exchange Commission and National Association of Securities Dealers regulations on managing e-mail and instant messages

have forced U.S. financial service providers to the forefront of adopting compliance practices. Other vertical industries have been equally affected. For example, within the U.S. healthcare community, the Health Insurance Portability and Accountability Act set the standards for securing the privacy of patient information.

A dynamic influx of U.S. and non-U.S. regulations and legislation – vertical and horizontal – has paralyzed busi-

ness activities. For example, according to a June 16, 2005, *Wall Street Journal* article, the cost of complying with the U.S. Sarbanes-Oxley Act of 2002 was then ranging from \$1.6 million to \$4.4 million per company each year. As a graduate student at the University of Rochester in 2005, Ivy Xiyang Zhang gained global media coverage of her event analysis of the July 2002 House and Senate debates over competing versions of the bill. Zhang postulated that the debates led to investor uncertainty resulting in falling stock prices and market losses of \$1.4 trillion.

However, the total cost of compliance for any mandate will differ wildly based on the type of analysis used. Undisputable, though, is the potential financial drain to become compliant, as well as the financial drain should an audit reveal areas of noncompliance.

Many argue that although the cost of becoming compliant is high, the upside is well-structured accountability,

At the Core

This article

- ▶ Describes the need to handle electronic communications for compliance
- ▶ Highlights the possible damage e-messaging can cause
- ▶ Offers suggestions for addressing messaging risks

improved organizational creditability, and customer protection. Capitalizing on that premise, vendors across-the-board have declared that they have the solution. In the case of e-mail and instant messaging management, the solution may take the form of policy-based filtering, categorizing, indexing, archiving, document management, or record management software – which turns the unstructured message body into a “record.” Outsourcers can host all or part of the solution. Professional services firms can design the implementation of the technical and business processes. The e-mail and instant messaging compliance market is undergoing tremendous consolidation; however, no vendor today can provide a holistic, integrated solution.

Privacy

Federal and regional privacy legislation dictates the degree of privacy required for customer- and employee-sensitive information. For example, student-record information is protected in many school districts. Communications held between an attorney and a client are protected as privileged information. Federal and local Freedom of Information Acts control the processes by which citizens can obtain government-held information about themselves. Organizations that wish to do business globally must understand how to get through the maze of complex and changing privacy mandates.

Civil Actions

Amid confusion about best practices to manage messaging for compliance, organizations must also mitigate the risks of civil lawsuits and corporate embarrassment – often initiated by employees exhibiting poor judgment. The following examples indicate the types of risk e-mail can pose to an individual or business.

Love on the Internet. In December 2000, Claire Swire sent a sexually explicit e-mail message to her boyfriend, Bradley Chait. Chait, a lawyer with the

Amid confusion about best practices to manage messaging for compliance, organizations must also mitigate the risks of civil lawsuits and corporate embarrassment – often initiated by employees exhibiting poor judgment.

London-based law firm Norton Rose, forwarded the e-mail message to several friends, who forwarded it to several of their friends, and so on. What Swire intended as a private message found its way, according to the media, to 10 million mailboxes across the Internet. Swire suffered personal embarrassment, to be sure, but beyond that, Norton Rose’s reputation was victimized by global ridicule because Chait forwarded the original message from his Norton Rose e-mail account. (Chait was suspended temporarily and his year-end bonus, along with those of nine of his friends, was revoked.)

Love Leads to Federal Indictment. The case of the *United States v. Kammerzell*, 196 F.3d 1137 (10th Cir.

1999) examines an incorrect method for dating. Utah resident Matthew Kammerzell wanted to spend some time with his girlfriend, who also lived in Utah. So Kammerzell used America Online (AOL) Instant Messenger (AIM) to send a bogus bomb threat to his girlfriend’s AIM account. His goal was to cause her office to close for the day so they could enjoy some time together. Kammerzell never imagined that he would be in violation of U.S. Interstate Commerce Commission (ICC) regulations, but his instant message traveled the Internet through AOL’s servers in Virginia. Kammerzell was indicted and found guilty of violating of ICC 18 U.S.C. § 875(c), which makes it a crime to transmit a threatening communication through interstate commerce.

Blog Transgressions Are Poor Career Moves. On January 28, 2005, Mark Jen was fired from Google because he discussed Google’s financial performance and future products in his blog. (Read Jen’s feedback at www.simplyfired.com/feature.php, in which he discusses the infamous blog *faux pas*.)

How Start-ups Fall Down. In 2005, the Canadian Imperial Bank of Commerce (CIBC) filed suit against Genuity Capital Markets, which was established by six former CIBC executives. The suit maintains that the former CIBC executives sent CIBC-confidential information via BlackBerry PIN-to-PIN messaging to improperly recruit CIBC employees to Genuity.

BlackBerry devices are each assigned a unique a personal identification number (PIN), and users can exchange messages with each other through PIN addressing (i.e., the sender and recipient are identified by each others’ PIN). Because PIN-to-PIN messages do not pass through a server, BlackBerry users may use it to send messages containing sensitive information under the misconception that PIN-to-PIN messaging cannot be captured and logged. But CIBC used PIN-to-PIN management software to capture the incriminating messages –

which were subpoenaed by the court to prove CIBC's case against Genuity.

**New Messaging Mediums:
New Risks**

Each new type of messaging invites a new level of casualness. For example, the language used in an instant message is generally less guarded than that used in an e-mail message. Behind casual communication lurks the danger of unintentionally or willfully providing information that should not be shared. Further complications can arise when different types of messaging intermix.

An e-mail message, which was intended to be viewed only by the sender and recipient, was posted by the recipient to a blog, an informal online journal. Worse yet, the blog posting of the e-mail message contained copyrighted material without the consent of the copyright owner. The sender requested that the blog entry be removed by the Internet service provider hosting it. (See www.chillingeffects.org/dmca512/notice.cgi?NoticeID=2093.) Although this example involves individuals, the blog posting could as easily have been a supposedly private e-mail message discussing an organization's intellectual property. In this context, legal liability issues are complex. (See www.eff.org/bloggers/ig/ for the Electronic Frontier Foundation's guidelines.)

Any messaging medium can carry incriminating information. In a proactive move, web conferencing vendors have started to release adjunct applications that capture, index, and archive specified content.

What You Need to Do Now

A messaging quagmire is underfoot in the majority of organizations. New messaging technologies are entering the organization at a grassroots level and at a faster pace than the IT organization or the business units can handle them. E-mail messaging and – increasingly – instant messaging, have come under unusual scrutiny. Organizations should expect that the same scrutiny will, over

Behind casual communication lurks the danger of unintentionally or willfully providing information that should not be shared. Further complications can arise when different types of messaging intermix.

time, be applied to other types of messaging. Implement some simple steps now to prepare for the inevitable.

- Clearly state in the organization's code of conduct that employees must follow the same ethical guidelines for professional behavior and communications, whether face-to-face or electronic.
- Rename the organization's e-mail policy "electronic communications" policy. Specific to ethics, it should reference the code of conduct. Additionally, the electronic communications policy should address such communications-specific issues as:
 - Spam. The policy should address

how the organization handles spam and the employee's responsibilities in curtailing it.

- **Message retention.** Retention handling will differ according to industry (e.g., financial services) and employee role (e.g., broker/dealers). Retention handling may not apply to some types of electronic communications (e.g., web conferencing) but will apply to other types (e.g., instant messaging). Discuss the implications of detailing which types of electronic communications are managed for retention with the organization's internal legal counsel and compliance officer.
- **Document and records management.** The policy should state whether the organization includes specific types of electronic communications (e.g., e-mail and instant messages) in their document management or record management systems.
- **Privacy.** Depending on the organization's geographical location (e.g., within a European Union country), legislative privacy issues may need to be addressed. Similarly, the organization's market sector (e.g., higher education) may need to address how message management is balanced against free speech – particularly for faculty (university employees) and students (not employees of the university).
- Do not include electronic messaging and communication etiquette in the electronic communications policy – which is a legal agreement between the employer and employee. Etiquette guidelines, however, can be referenced in the policy document.
- Evaluate product selection decisions against market trends, short-term needs, and strategic goals. Messaging management point products are

converging – often as a result of acquisitions. A number of industry businesses have been merged or acquired in the past two years.

- Educate employees; this is paramount. It is the responsibility of employees to think before they type – if it feels wrong, it probably is.
- Seek the advice of internal legal counsel and compliance officer before implementing any business practices or policies. ■

Editor's Note: This article is based on an article that first appeared on the website for Grey Consulting (www.grey-consulting.com) and on a presentation the author made at the ARMA 2005 conference in Chicago.

***Maurene Caplan Grey** is the founder and principal analyst of Grey Consulting. Her research focuses on messaging and collaboration. Before starting an independent practice, Grey was Gartner's lead analyst on messaging, calendaring/scheduling, and human communications. Earlier, she headed United Parcel Service's global messaging environment. With more than 20 years in the IT space, Grey is recognized within the vendor community as a subject matter expert in messaging. She also serves on ARMA's Standards Development Committee task force developing a publication on records management issues in collaborative environments. She can be reached at maurene.grey@grey-consulting.com.*

References

Bialik, Carl. "How Much Is It Really Costing to Comply With Sarbanes-Oxley?" *Wall Street Journal Online*, 16 June 2005. Available at <http://online.wsj.com/public/article/SB111885041027560378.html> (accessed 26 September 2006).

Xiying Zhang, Ivy. "Economic Consequences of the Sarbanes-Oxley Act of 2002." Ph.D. diss., University of Rochester, 2005. Available at http://w4.stern.nyu.edu/accounting/docs/speaker_papers/spring2005Zhang_Ivy_Economic_Consequences_of_S_O.pdf#search=%22Ivy%20Xiying%20Zhang%22 (accessed 26 September 2006).