Balancing Privacy and Risk in the E-Messaging World

Dianne Solomon
First Data

Messaging within an enterprise used to be like the local water department; as long as the email flowed, no one paid any attention to it and all was good. Things are different now—messaging has become the center of a legal and regulatory maelstrom. It's the confluence of security, privacy, and opportunity within an organization. Email and instant messaging reduce the cost of delivering products, increase responsiveness to customers, enfranchise distance expertise, and evenly balance employee work/home responsibilities. Yet, these very same technologies open the door to intellectual property loss, malware intrusions, employee harassment, and compliance violations.

Messaging risk comes in many flavors: compliance requirements, privacy, domestic and international law, and unique technical considerations. As with any other risk assessment, organizations must weigh compliance costs against probability and magnitude of impact. In this article, I'll take a look at some of the more significant legal and regulatory drivers and illustrate what risk might look like within an organization. I'll then show the controls that organizations can apply to meet legal and compliance requirements and mitigate risk. As with all other security assessments, organizations should share this information across disciplines within the company so that the resulting plan reflects the collaborative thinking of security, legal, human resources, privacy, and business professionals.

History and regulations

The legal and regulatory environment that influences messaging is fairly new and continuously evolving. Laws, regulations, and court decisions raise questions for organizations about what they should permit, transmit, and store.

Internationally, the European Union (EU) was among the first to regulate electronic content with the 1995 EU Data Protection Directive. The EC approved Safe Harbor in 2000, creating a framework under which US global organizations can certify compliance. Domestically, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule also went into effect in 2000. It regulated the use and disclosure of personally identifiable health information. In 2003, the US Congress promulgated the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), which regulates commercial email content.

Case law evoking US Federal Equal Employment Opportunity laws and the findings of the US Office of Special Counsel continuously expand the scope of protections that businesses must provide to ensure harassment-free workplaces. According to a 2004 survey conducted by the American Management Association and the ePolicy Institute, 21 percent of the businesses surveyed had had e-messages subpoenaed; another 13 percent had faced legal challenges related to employee email.[1]

Nothing points more dramatically to the growing interest in electronically stored information or the cost of producing messages for litigation than the amendments to the US Federal Rules of Civil Procedure that went into effect in December 2006.[2] Changes to a dozen or more federal rules established that electronically stored information qualifies as business records and is to be included in litigation discovery.

Privacy

Private data—commonly called *personally identifiable information* (PII)—are pieces of information that uniquely identify an individual. Although international, federal, and local laws vary in definitions, it broadly includes

- an individual's full name, address, telephone, or fax number;
- dates such as a birth, admission, or discharge date;
- national identification, certificate, or license numbers;
- medical record, account, or student ID numbers;
- photographs or biometric identifiers; and
- credit-card and card-verification numbers.

In addition to PII, businesses and organizations also have information they consider private. It's typically classified internal, confidential, or restricted, and includes information such as pre-release financials, audit reports, salary information, and pending patents.

Privacy requirements related to outbound messaging strive to ensure that private information is transmitted only when necessary, with the individual's knowledge and consent, properly secured, and to the appropriate recipient. Privacy requirements can also relate to inbound messages such as protection from phishing attempts and other means of persuading individuals to disclose private information. Physical requirements address what's to be done with printed messages to prevent dumpster diving (looking through trash bins for printed messages) and shoulder surfing (looking over an individual's shoulder as he or she receives confidential messaging content).

Organizations need technical controls and security policies to protect private information. To start, they must know what type of content traverses their messaging networks. For example, does the organization send out system-generated customer reports that include account numbers? Does it use email to send employment offer letters or medical test results?

Policies must clearly identify the information that shouldn't leave the company and what can leave if properly secured. Organizations should also address employee behaviors such as mailing confidential business information to home email accounts or leaving printed messages with private information on copiers or fax machines.

With policy-based controls in place, organizations can start looking at technical controls, including

- access controls around source data;
- content filters that block, capture, or report on prescribed content;
- secure Internet-bound messages;
- forensically sound archives for message copies; and
- limited access to personal email and instant messaging accounts.

It's important to keep in mind that user-generated content will always be one step ahead of technical controls. Therefore, organizations can't underestimate the value of continuous education and rapid responses to policy violations.

Workplace issues

An organization's human resources department typically addresses workplace issues such as employee–manager disputes, harassment claims, and wrongful termination. E-messages supporting these issues can be items such as requests for time off and any responses, discussions about employee performance, and inappropriate content (jokes, language, images) sent or received.

Organizations won't know which messages are of interest until a workplace issue surfaces and restored messages are requested. But how long should a company keep backup and archive copies, and in what format?

Two kinds of message archives exist. The first resides within the messaging system, sitting on a server, a locally stored file, or a backup tape. These files are difficult to control and costly to search. They also provide little granularity, forcing the organization to save all or nothing, based on an arbitrary date, storage capacity, or restore ability.

The second type of archive sits outside of the message system and automatically captures every message that routes through it. Messages are captured individually rather than as part of a mail file or collection of files. These systems can be forensically sound, showing proof that the content wasn't altered, and they support sophisticated search and retrieval so that organizations can thoroughly research issues that surface.

Litigation

When we look at financial vulnerability in messaging, there's no greater sore spot than litigation. Whereas courts used to look for a smoking gun, they now look for the smoking message—and the costs related to finding, searching, and producing it can run into the millions of dollars.

Once an organization knows a matter is of interest, it's obligated to move quickly to discover all relevant messages and produce them in a forensically sound format. If the matter is complex, the job of identifying relevant messages and weaving their content into evidence can be profoundly burdensome.

The recent amendments to the US Federal Rules of Civil Procedure introduced a new term—electronically stored information—and attempts to constrain the burden of e-discovery in civil matters. Because the key concept is electronic information that the organization stores, the natural question becomes, "What should the organization store?"

As electronic-based communications grow (instant messages, voice mail, voice over IP [VoIP], and so on), the organization must decide if it wants or needs to retain those files. Legal and IT professionals will have to keep an eye on growing trends in retention and lit-

Whereas courts used to look for a smoking gun, they now look for the smoking message—and the costs related to finding, searching, and producing it can run into the millions of dollars.

igation to decide if or when the exposure of not preserving these new formats exceeds exposure for maintaining them.

The best safeguard is to educate your staff on CAN-SPAM Act provisions so that compliance is built into all projects and contracts related to email services.

The CAN-SPAM Act

The US Congress promulgated the CAN-SPAM Act of 2003 to ensure that commercial email's source or content isn't misleading and that recipients can refuse to receive the email if they so choose.[3] The law's scope, however, can impact any organization that sends out commercial email. Key provisions of the CAN-SPAM Act include

- subject lines can't misrepresent message content and ads are identified as ads;
- senders must provide a valid return email address that's active for at least 30 days, as well as a valid postal address;
- messages must include an opt-out mechanism, and senders must act on requests within 10 business days;
- senders must maintain an opt-out address list that accompanies the distribution list if sold;
- senders can't create distribution lists from harvested addresses or by electronically generating address permutations;
- email must transit legitimate messaging systems, not open relays or unsuspecting computer systems;
- senders can't use email to commit crimes such as distributing child pornography, fraud, or introducing viruses, worms, and Trojan code into other computers; and
- header information must accurately identify the sender.

For legitimate businesses trying to comply with the law, the security challenge to ensure that all of their electronic products are compliant. If other workgroups create and distribute email, they might not be fully aware of the requirements. Typical violations include

- contracting with a messaging-distribution system that sends email under your domain name. Recipient spam devices could reject the emails because of the header mismatch. Messages rejected as spam don't generate nondelivery notifications, leaving the workgroup unaware of the nondelivery;
- failure to share opt-out addresses across different workgroups that send mail under the same corporate address or IP address; and
- termination of return email addresses less than 30 days from the last mailing.

The best safeguard is to educate your staff on CAN-SPAM Act provisions so that compliance is built into all projects and contracts related to email services.

Global enterprise messaging

If you work in the US and send an email using your company's PC and messaging system, your company has the right—and in some cases an obligation—to ensure messages don't violate the protections it owes its customers, employees, and shareholders. Storing a copy of every message in a secure repository is encouraged. Employees are advised to hold no expectation of privacy with regard to what they send or receive.

However, if you work for that same company but sit in an EU member nation, the balance between privacy and business is quite different. There's a presumption that your mail is private unless there's a compelling reason for disclosure. Backup and failover systems might be prohibited if placed outside of the originating country, out of concern that access controls don't meet the same privacy standard.

So how does this affect the global enterprise? Using email to collect and share information necessary to support administrative functions might be prohibited or restricted, and electronically transmitting employment records from one region to another might not be permissible. These and other privacy safeguards can significantly impede an organization's efforts to reduce duplicative processes in multiple locations.

There's no easy answer to how organizations can meet local privacy requirements while centralizing administrative functions, but there are certain approaches that work toward that, such as the EU-approved Safe Harbor framework. Under Safe Harbor, US companies can certify compliance with EU privacy directives. This keeps EU courts from continuously scrutinizing a company's privacy practices. However, the EU isn't the only state with strict privacy guidelines. Argentina, Australia, China, and New Zealand are just a few countries that insist on business compliance with privacy guidelines. US organizations with international offices will need to understand the local requirements to avoid business delays, court challenges, and other related message-content risks.

E-messaging risks aren't limited to traditional IT concerns. Everyone—from customers to shareholders—has a vested interest in message content. Organizations need policies to dictate what gets sent, saved, transmitted, and restored. Yet, policies that best support one group within the organization are often at odds with other groups. There is no one "right" answer. However, no risk assessment of the messaging environment is complete without an open discussion with all of the players.

So is that it? Hardly! E-messaging's scope is growing daily. New technologies such as instant messaging and VoIP are becoming common place in the corporate world and will inevitably become the subject of e-discovery. The changing workforce, including home-based users, the proliferation of wireless metropolitan area networks, and the shift of outsourcing from India to Japan, will present new threats and privacy challenges. At the same time, these same technologies and these workers will be developing new products and services distributed over the e-messaging networks. It's an exciting time, but a risky one. □

References

1. Am. Management Assoc. and the EPolicy Inst., *Workplace Email and Instant Messaging Survey Summary*, 2004; www.epolicyinstitute.com/survey/survey04.pdf.
2. *The New E-Discovery Rules*, Dahlstrom Legal Publishing, 2006.
3. *The Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003*, Public Law No. 108–187, *US Code*, Title 15, sections 7701 et seq.; www.spamlaws.com/pdf/pl108-187.pdf.

***Dianne Solomon** serves as messaging security officer and technology privacy officer at First Data, and is pursuing graduate studies in information security at Nova Southeastern University. Her research interests include e-message security, content control, and privacy in the global enterprise. Solomon has an MLS from Rutgers University School of Communication, Information, and Library Studies and is a member of the International Association of Privacy Professionals. Contact her at dianne.solomon@firstdata.com.*