Information Management

Protecting the Once-'Silent' Record:

E-MAIL

Cherri-Ann Beckles, Ph.D.

From an early stage of the digital age, the use of electronic mail (e-mail) has been an integral part of communication within public and private organizations. With the emergence of the Internet, it also quickly became a means of global communication, surreptitiously replacing the traditional letter and memorandum as a quick and easy way to communicate.

Initially, organizations treated e-mail as ephemeral. Its ownership was blurred as e-mail accounts did "double duty," in many cases, becoming a blend of mission-critical information and decision-making with personal opinions and informal rhetoric. There is evidence that this has not yet changed across many types of organizations despite e-mail's profound impact on organizational management and individuals.

Many organizations acknowledge that e-mail can no longer be treated casually, particularly in today's litigious and politically charged environment. The true "recordness" of e-mail must be fully explored as a separate and distinct area of study in the discipline of records management. This article examines the brief but profound history of e-mail as a record (see sidebar on page 41) and how organizations through the years have dealt with what has been referred to by some as "the e-mail problem."

E-mail as a Record

To fully recognize the magnitude of the e-mail problem, it is important to first understand how e-mail works. To a layperson, e-mail appears to leave the outbox and take a straight path to the recipient's inbox. However, this is not the case.

From a records management perspective, here is the lifecycle view of e-mail:

- Creation stage: A message is composed or created by the mail client.
- Distribution and use stage:
  - The simple mail transfer protocol consults a domain name server (a type of Internet address book) to map the exact location of the mail exchange server.
  - The message is sent to the designated mail exchange server, but it may be sent to six or more virtual locations before reaching its destination.
- Disposition stage: The e-mail is accessed by the receiver, who determines its final disposition.

It may be argued that sending an e-mail results in the creation of a record from the point where the e-mail leaves the outbox and is recorded as "sent," and here is why. Electronic records are fluid in structure, but they still qualify as records if the associated metadata, or data in the e-mail about the e-mail (context) and content remain unchanged, and the integrity of the systems used to create, distribute, and store them is reliable. The content and structure must be preserved without any kind of manipulation throughout transmission. So, the e-mail and it attachments can be properly classified as a record because – despite its movement through various points to its destination – the associated metadata remains static.

The E-Mail Problem

If an e-mail record is not intended to be disclosed except to the parties involved, it is vulnerable to unwarranted access. And, because sending e-mail results in copies existing in more than one virtual place, it is difficult to erase or "forget" them as evidence, even if they are deleted by the sender and the receiver.

E-mails are considered evidentially sound and admissible in the court of law because their associated metadata state unequivocally the sender, date sent (timestamp), and the recipient, leaving no question of what was written, by whom, and

when and where it was intended to be sent. One of the early U.S. court cases that affirmed e-mail as a record, *Kasten vs. Doral Dental USA, LLC,* took place in 2007, when the Wisconsin Supreme Court ruled that business-related e-mails were "company documents" and not just mere private communication.

Protecting the E-mail Record

The full unpleasantness of uninhibited e-mail record creation and distribution is coming to the fore in this age of cybercrime and cyber bullying, and it was on full display in the 2016 U.S. presidential campaign. On July 25, the *Washington Post* exposed information from e-mails originating from key people on the Democratic National Committee (DNC), including its chair. These e-mails provided evidence of unfavorable activity and led to the DNC chair's removal and other unwelcomed events. This clearly demonstrates the power of the e-mail record, even in today's fast-paced, information-sharing age.

E-mail phishing, hacking, spamming, spoofing, and bombing are but a few terms that are used in today's digital environment to describe mainly criminal acts against e-mail users; their rights and liberties, including their right to privacy, are under assault by cyber criminals. Beyond the threat to individuals, organizations are threatened by breaches of confidential information when e-mail is not properly administered. These are serious and negative outcomes that could result in public embarrassment and financial loss.

Information professionals must keep abreast of rapidly changing technologies to counteract new forms of cybercrime, prevent the loss of institutional memory, and meet the information governance objective of promoting transparency and accountability in all forms of information.

Key Mechanisms for Protecting E-mail

Records management practitioners must safeguard their organizations and customers through establishing appropriate e-mail policies, procedures, and other mechanisms that may be technical in nature, such as those that follow.

E-mail Policies

E-mail policies are critical control documents that provide guidance to employees on the appropriate and inappropriate use of organizational

A Brief History of E-mail

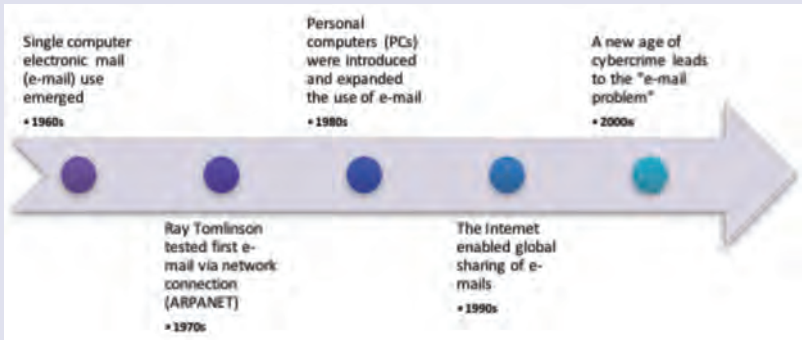

Figure 1: E-mail History Timeline

A description of the origin of e-mail is dependent on how the term is defined. As pointed out by the University of Maryland's "A Brief History of Email," if e-mail is defined as "messages transmitted electronically," it would include Morse code. If defined as the Oxford English Dictionary does as "messages distributed by electronic means from one computer user to one or more recipients via a network," it suggests a network of computers must be involved. In the latter case, programmer Ray Tomlinson can be credited with sending the first e-mail via an experimental file transfer protocol called CPYNET in 1971.

He had made improvements to a 1960's inter-user mail program called SNDMSG, allowing users to compose, address, and send a message to other users' mailboxes. In addition, Tomlinson provided a way to distinguish between local and network mail by using the symbol "@" and a host name. He was then able to send test messages to himself using a network called ARPANET. That was the beginning of network e-mail. An updated file transfer protocol soon replaced CPYNET, and the use of the ARPANET, which was a forerunner to the global Internet, was further developed by the U.S. Department of Defense.

A revolutionary phenomenon of the late 1970s and 1980s further drove the development of e-mail communication: the advent of personal computer systems, namely the IBM personal computer (PC) and Apple Macintosh, which used "bulletin board systems" to send and receive messages. The PC was sold by the hundreds of thousands and its use soon expanded from the military and into governmental agencies and public and private companies and organizations. Workers began exchanging messages uninhibitedly via intranets or local area networks (LANs). LAN-based systems were favored because of their ease of use and ability to send and receive attachments. By the mid-1990s, the Internet led to another phase in the development of e-mail by enabling global access to shared information.

Within four decades, the emergence of enabling technologies and devices propelled e-mail communication into one of the most popular and accessible means of public and private communication. Unfortunately, attention given to the security of data lagged, and the "e-mail problem" of the new millennium began to rear its ugly head.

Read More About It

Blake, Aaron. "Here are the latest, most damaging things in the DNC's email leaks." *The Washington Post*. July 25, 2016. Available at *www.washingtonpost.com/news/the-fix/wp/2016/07/24/here-are-the-latest-most-damaging-things-in-the-dncs-leaked-emails/?utm_term=.f32ea6b88212.*

McKemmish, Sue, Michael Piggott, Barbara Reed, Frank Upward. *Archives: Recordkeeping in Society*. New South Wales: Chandos Publishing, 2005.

Orman, Hilarie. *Encrypted Email: The History and Technology of Message Privacy*. Springer International Publishing: New York, 2015.

Raytheon BBN Technologies. "The First Network Email: A History from Ray Tomlinson," 2011. Available at *www.raytheon.com/news/rtnwcm/groups/public/documents/content/rtn12_tomlinson_email.pdf.*

University of Maryland. "Brief History of Email," 2002. Available at *www.cs.umd.edu/class/spring2002/cmsc434-0101/MUIseum/applications/email-history.html.*

Wall, David. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press, 2007.

e-mail. RIM practitioners should work collaboratively with IT and other key managers to formulate a comprehensive policy that includes rules for e-mail retention and disposition, e-mail security, and privacy controls, among other requirements. The policy should be well communicated to all staff members.

E-mail Encryption, Authentication

One means of protecting e-mail is by using cryptography. These forms of protection are called encryption and signing by using digital signatures. End-to-end encryption, as used by Whatsapp, is one of the strongest forms of e-mail protection. It allows the sender to encrypt the message that can be decoded only by its final recipient.

E-mail Management via EDRM Systems

Organizations with robust electronic document and records management (EDRM) systems should ensure that all business-related e-mails are captured and categorized in logical classification schemes with adequate security matrixes. This will prevent unwarranted access to e-mail records by unauthorized persons. The correct retention and disposition periods should also be instituted within the EDRM system.

Confidentiality/Privacy Statements

Confidentiality statements should be appended to organizational e-mail stating that the content of the e-mail is legally protected and strictly prohibiting unintended recipients from copying, storing, or otherwise disseminating the e-mail or attachments.

Awareness and Training

It is imperative that organizations seek to raise awareness about the uses and dangers of e-mail. E-mail policies should be properly communicated to all levels of staff. New and existing staff should be trained in e-mail etiquette and how to create e-mail as a business record.

The Need for Research

E-mail messages have been silent records over the last 50 years, documenting and providing reliable evidence of activity through metadata and e-mail threads in an inconspicuous way, but with implications for the future as archival records.

E-mail and other newer forms of electronic communication, such as instant messaging, social media, and blogs, that result in fluid records pose challenges to records managers and archivists worldwide. It is therefore imperative that in-depth research is carried out within the disciplines of records and archives management that will further investigate the "recordness" of online communication and the results of this type of record creation over time.

This research will better prepare records and archives practitioners to understand the impact on governments, organizations, communities, and individuals at present and in the future in the quest to find meaningful solutions to protect confidentiality and privacy while ensuring that valuable, researchable information is preserved for posterity. E

About the Author: Cherri-Ann Beckles, Ph.D., is the assistant archivist at The University of the West Indies (UWI), Cave Hill Campus, Barbados, where she is also a lecturer in its records management certificate program and an assistant lecturer in an archives and records management module of its masters in heritage studies. Beckles has also worked as an archives and records management consultant throughout the Caribbean region for the last 12 years. She holds a master's degree in records and archives management from the University College London, a master's degree in history from UWI, and a Ph.D. in archive and information studies with a focus on information rights at the University of Dundee, Scotland. Beckles can be contacted at *cabeckles@yahoo.com*.