Implications of E-Mail Mismanagement and Best Practices for Preventing It

John Isaza, Esq.

E-mail mismanagement continues to make headlines almost daily. In this article, California-based attorney John Isaza answers several questions about e-mail best practices and the legal repercussions of poor e-mail management in the United States – because bad press can be costly to any organization.

In the United States, could a person really go to jail for destruction of e-mails?

In short, yes. However, at the U.S. federal level, the punitive provisions under the Sarbanes-Oxley Act are rarely cited or used, and even so, they are limited to federal investigations and don't apply to court cases.

Should the courts ever choose to entertain it more regularly, culprits could face jail time or millions of dollars in sanctions under the little-utilized 18 USC Section 1519 (Destruction, alteration, or falsification of records in Federal investigations and bankruptcy), which states:

> Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

Fines in the millions and the specter of 20 years in jail are serious business. The questions, thus, become:

- To what extent can an organization destroy information if it knows it is not relevant to an investigation?
- Should the organization, instead, preserve information to avoid the appearance of impropriety?

Ultimately, the choice to delete e-mails during pending or threatened litigation or agency investigations is a risk-based decision that organizations with multiple legal holds have to entertain on a daily basis. Among the questions to ponder is "Can an organization delete, say, disaster recovery tapes that include e-mails, even if there is pending or threatened litigation?" To answer that question

affirmatively, the organization must be absolutely certain that the tapes are purely redundant for disaster recovery only and don't constitute their *de facto* records management system.

With the above as a backdrop, following are some related areas of concern.

What are some best practices in encouraging – or compelling – the deletion of old e-mails?

All these issues go the core tension between records retention and the need to dispose of expired data. If the information exists and is relevant to the subject matter of a lawsuit or investigation – even if it is merely anticipated or foreseeable litigation – it is discoverable. Therefore, it behooves organizations to dispose of needless e-mails and data *before* litigation/investigation ensues or becomes credibly probable.

If a *record* – which ARMA defines as "any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business" – has expired according to the organization's retention schedule, it should be disposed of immediately, unless, of course, it is subject to a legal hold at the time. Otherwise, the organization opens itself up for liability and discoverability of e-mails that could be read out of context.

The real trick for organizations is to determine which e-mails are *records* that must be retained per the retention policy, versus all other non-record data that can be disposed of at any time as long as it is not subject to a legal hold.

Are there any cybersecurity repercussions for comingling personal and work e-mail accounts?

Attempted breaches of mobile devices are on the rise, especially considering that most mobile devices include e-mail accounts. In the first quarter of 2012, for instance, McAfee Labs recorded more than 8,000 mobile malware strands, with the vast majority seeking to penetrate Android systems. This was a 400% increase over the previous year, according to Visage Mobile's white paper "Lighting the Path to Successful BYOD Programs."

Thus, the seriousness of a potential breach is palpable, especially in the case of a government official or corporate officer accessing personal e-mails on a mobile device, which could have less secure connections than official state business accounts.

If an e-mail account is hacked, does it put all the people in the organization using the server at risk?

Not necessarily. The security risk depends entirely on such things as the type of hacking, the target, its breadth, and the content accessed. Hacking into a person's e-mail account does not necessarily mean access to his or her e-mail contacts, though it could be damaging to the extent that any of the contents could be discerned from the e-mail account. It would depend on how the account is configured and what kind of integration it has with other devices, such as the person's laptop, office computer, iPad, and cloud-based servers.

Is there required self-reporting if an e-mail account is hacked?

Depending on the organization's industry, a hacking incident may be subject to requirements to notify government authorities, third-party associates, and customers. Basically any organization housing personally identifiable information (PII) or payment card industry (PCI) regulated data could be subject to disclosure requirements and, by extension, so would the individuals of that company.

In the healthcare sector, for instance, data breaches are a serious event that would trigger all kinds of regulatory scrutiny. On the opposite end of the spectrum, even organizations that are not in a highly regulated PII or PCI environment need to vet all breaches.

All organizations' BYOD policies should include language requiring employees to notify them about any breach of their personal devices. Depending on the size and industry of the organization, it might also provide a reporting hotline.

How can organizations find out if an executive is using personal e-mail accounts for business?

Typically, the use of personal e-mail accounts is discovered during routine audits. However, since audits may be infrequent or audit recommendations ignored, it may take an embarrassing event to bring attention to the issue for some organizations. At its core, the biggest problems arise from the ever-increasing use of personal devices in the workplace and with employees logging into work from their home computers or laptops.

Although the BYOD issue has been on the radar of most large organizations for the last three to five years, they are succeeding in setting policies around it only to varying degrees.

Presumably, the BYOD policy will stress that personal e-mail accounts are never to be used for business. In practicality, though, this can be a challenge to prevent. When a device has both business and personal accounts attached to it, for example, it is easy to erroneously send a work-related e-mail from a personal account. Once that happens, if the recipient replies to all, the stage is set for a breach in the BYOD protocol.

What are some good tips for an organization to prevent use of personal e-mails or applications for business purposes?

All organizations should have BYOD policy, procedures, and guidelines that include five core elements:

1. Guidance on acceptable uses of personal devices to transact official business, including instructions on distinguishing personal e-mail account usage from official business accounts
2. A list of the types of sanctioned devices (e.g., iPad, Blackberry, iPhone) and rules of engagement with IT
3. Policies around logistics, such as whether the company will reimburse for usage of the personal device
4. Security information that addresses encryption and other features that must be enabled to protect the data in the event of a loss or breach
5. A section on risks, liabilities, and disclaimers to help protect the organization against the employee misuse of the device

Armed with the BYOD policy, other organizational documents (e.g., policies for password usage, cloud computing, social networking) could get into the specifics of training and auditing for compliance, including the frequency for these.

Who is at fault for user violation of e-mail protocols?

Ultimately, progress and the competition to stay on top of the competition are at fault for e-mail protocol violations. The adoption of technology has far outpaced the ability of organizations to keep up with the implications of using it. Consumers and customers demand the immediacy facilitated by technology, so people, processes, and procedures take a back seat in favor of adoption.

In the ideal scenario, before organizations roll out or permit any new technology (e.g., e-mail tools, social media, content management), they need to vet their change management process (i.e., a controlled roll-out that ensures proper user adoption and compliance), as well as their ability to audit and monitor compliance with their policies and procedures. In today's fast-paced world, constant auditing and monitoring are required.

Those looking for "fault" are looking at those who do not learn from their experiences. In those instances, those in charge of the program roll-out are at fault for not paying attention to system failures.

All that said, a corporate leader confronted with a systematic policy failure, coupled with high-level customer demands to keep up with technology, faces a losing battle. The key is to strike a balance between controls and business needs. **END**

John Isaza, Esq., can be contacted at *John.Isaza@InfoGovSolutions.com* or *John.Isaza@RimonLaw.com*. See his bio on page 47.