This is part of a syndicated column I have created for ARMA chapters, including the Phoenix Chapter of ARMA Newsletter. My column is devoted to answering information governance, records management and related legal questions from Chapter Members. As you read my responses, please note that although I am an attorney specializing in these areas of law, these are only my opinions based on very limited knowledge of the Member's particular circumstances. My opinions should not be construed as legal advice. Kindly consult with an attorney for more formal advice. That said, please keep your interesting questions coming.

1) The social media space has exploded over the last 10 years. Of all different types of social media such as Facebook, Twitter, Second Life, etc., that are finding their way into the business world, if an organization had to pick one platform to focus on first for Records & Information Management, which one would you recommend they address first (and why)?

   The answer depends on which medium the organization uses as a vehicle to promote its services. For instance, if the organization has a formal presence on all three media, then all three need to be managed simultaneously. Prior to establishing a presence, the organization should have established policies and procedures to govern the interaction within the medium. As far as control of usage of the media for personal reasons, accessed through company technology, then one policy could put this issue to rest. This policy could specify the limited use of the systems for personal purposes or simply prohibit access from company devices. The policy also should forbid commentary about the company in personal social media, and specify that all commentary, if any, must be vetted through the organization's formal presence. Most of this is easier said than done, so a change management strategy should be considered. The limits of this column do not allow me to go into more detail. Suffice it to say that this response addresses only the tip of the iceberg.

2) "Defensible Destruction" is a hot buzzword right now.
   a. In the context of hardcopy records, what can organizations do to create defensible destruction process for their legacy hardcopy records?
   b. In the context of shared drives, what are key factors for an organization to consider to create a defensible process?
   c. Do you see any potential big wins in organizations attempting to clean up their structured data?

   The first thing that comes to mind as the most obvious vehicle to establish a defensible destruction process for all of the above is to follow the GARP® principles. From there, the key to defensibility is to have an established process that has been engrained in the organization's routine and good faith business processes. Ultimately, even if the process is not perfect, courts should be eager to give the organization the benefit of the doubt for at least following a process that is agnostic to any particular lawsuit or investigation.

3) The sheer number of data security breaches each year is overwhelming. What are some of the key breaches you've seen?

A couple immediately comes to mind. In the July/August 2011 issue of *Information Management*, the following was reported at page 19:

> "In what may be the largest U.S. data breach to date, hackers gained access to the client files of online marketing provider Epsilon in April [2011]. Those files contained customer information supplied by many large U.S. retailers and banks, including Best Buy, Walgreens, Citigroup, and JPMorgan Chase… The good news for consumers is that no personally identifiable information (e.g., account or credit card information) was accessed."

Epsilon dodged a major bullet, as no personal information was hacked. Had that been the case, the result could have threatened the future of the organization as an online marketing provider. Even so, the event was terribly embarrassing to the organization.

Another major data breach did involve the personal information of 3.5 million Texans, including names, addresses, birth days and social security numbers. The Texas government's data was made available on a public server for longer than one year. Although the data breach did not involve hackers or even disgruntled employees, it was passed around various state agencies culminating in a state-controlled public server. *See Information Management*, July/August issue at page 16 (Volume 45, No. 4).

4) What are 2 things companies can do to protect themselves from security breaches?

It is not possible to enumerate only 2 things, without knowing the state of the organization, its business priorities, and its current systems. However, at the risk of beating a dead horse, I return to assessing your preparedness under the Principle of Protection of the GARP® principles. The organization needs to give itself an initial score under the Maturity Model. Then, it should determine from there what steps must be taken to reach the desired level of compliance, which should be a minimum of level 3, if not higher, depending on the sensitivity of the organization to protection issues and breaches. For an online marketing company, such as the one mentioned in response to Question 3, a level 5 may be the desired level of compliance under the principle of Protection.

John Isaza is a California-based attorney and Partner of RIMON Law Group, PC, a twenty-first century law firm that includes specialty in electronic information governance, records management and overall corporate compliance. He may be reached at John.Isaza@RIMonlaw.com or follow him on Twitter and LinkedIn.