Information Management

The Case for
Including RIM in Information Security

Andrew Altepeter

The debate about the best organizational placement for the records and information management (RIM) function is perhaps as old as the profession itself. The profession has continually needed to reinvent itself, and with less attention and fewer resources being given to traditional RIM than perhaps ever before, the debate is as important as ever.

One approach to gaining resources and raising the RIM program's profile has been to widen the scope of RIM into the discipline of information governance. This article offers a similar, though distinct, approach: to strategically align with another function that is highly valued in an organization – in particular, with information security (IS).

Why the Org Structure Matters

Where a RIM program sits within an organization has tremendous implications for its ability to add value, reach its goals, and achieve success. Most importantly, its placement needs to ensure executive sponsorship and program visibility.

Aligning the program with an executive whose priorities overlap with traditional RIM principles results in a win-win for the program and the organization. Being in the right place enables the RIM program to leverage the organization's resources: tools, people, and dollars. When the program enables management to deliver results, gaining RIM program funding will no longer be an uphill battle.

The Best Placement for RIM

With regards to organizational alignment, there is no single, perfect fit for RIM. The most common placements are with shared services, finance, legal, or IT. Reasonable arguments can be made for choosing any of these functions, but the best choice depends on an organization's leadership's priorities, legal and regulatory profile, and the information landscape.

For example, a RIM department in a company operating in a highly litigious business environment may benefit from being placed in the legal group. Resources will be abundant, and RIM will be seen as a key business partner in helping the company protect itself in the e-discovery process and in court. Placing RIM in the finance department of a major financial services firm may offer similar benefits.

A RIM program that is already strategically aligned and flush with resources and visibility should stay there; there is no need to fix what isn't broken. In many cases, though, the placement of RIM seems to be an afterthought. Given recent developments in technology and the rise of cyber threats, pairing RIM with IS may be the best choice, offering strategic benefits to the organization and to the RIM and IS programs.

It is worth examining the potential benefits of this alignment to both programs, taking into consideration the areas where the RIM and IS programs' objectives overlap.

Common Principles for RIM, IS

One of the more commonly stated goals of an IS program is to ensure the protection, availability, and integrity of an organization's most important information assets. These goals probably sound familiar to readers, as they are also counted among ARMA's Generally Accepted Recordkeeping Principles® (Principles). In fact, a closer look shows quite a bit of overlap with several Principles, the following being the three most significant ones.

Principle of Integrity

The Principle of Integrity states, "An information governance program shall be constructed so the information generated by or managed for the

organization has a reasonable and suitable guarantee of authenticity and reliability."

Integrity flows from proper protection. Ensuring information is protected from malicious access means it cannot be destroyed or manipulated and provides a reasonable assurance of its authenticity and reliability. RIM and IS both have always had a role to play in this.

Principle of Protection

The Principle of Protection says, "An information governance program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, classified, or essential to business continuity or that otherwise require protection."

This goal is foundational to any IS program. The chief information security officer (CISO) will certainly already be familiar with the need to:

- Develop an information classification schema whereby information is labeled as public, internal, or confidential
- Apply proportionate controls to protect sensitive data
- Put in place auditable access controls, as well as logging and monitoring mechanisms to ensure proper protection is taking place

The majority of security tools deployed in a given environment are dedicated to protecting sensitive data.

Principle of Availability

The Principle of Availability says, "An organization shall maintain records and information in a manner that ensures timely, efficient, and accurate retrieval of needed information."

IS plays a vital role in maintaining critical information availability. If this information is not available to the business, it will ultimately fail. Protecting against cyber threats, such as denial of service or distributed denial of service, is critical to maintaining system availability. In addition, IS programs are often responsible for maintaining disaster recovery and business continuity services.

Possible Benefits to IS

RIM brings strategic benefits to any IS program. First, a RIM program brings knowledge of:

- Data flow
- Where sensitive data and systems sit in the organization

…RIM may have established processes that IS will be able to use as a model for creating or improving its own processes to become more efficient and save resources.

- Who has access to what information
- What data may contain personally identifiable information (PII) and be subject to additional regulation
- Potential new repositories of information that lack sufficient protection, which is critical to a CISO determining where to deploy limited resources

Secondly, RIM is able to act as a key partner by advising on retention rules, including for sensitive data across the organization. Properly applying retention to information has benefits beyond satisfying legal and regulatory requirements. If retention is correctly applied and information past its retention date is securely disposed, the threat exposure, and thereby the overall risk to the organization, is decreased. Reducing the volume of information will also allow IS to deploy its resources more efficiently.

Lastly, RIM may have established processes that IS will be able to use as a model for creating or improving its own processes to become more efficient and save resources. For example, rather than RIM and IS having separate compliance training courses or audits throughout the year, IS may be able to add RIM-related content to its own and reduce overhead.

Possible Benefits to RIM

Information security is top of mind for all executives for organizations that have sensitive information, such as PII and intellectual property. Compromise of this data can prove catastrophic, as attested to by the numerous articles reporting on the significant financial and reputational damage suffered by organizations whose data has been breached over the past several years.

IS departments have been the biggest beneficiaries of these unfortunate events, as organizations globally are increasing security budgets, staffing, and tools in response to them. Landing in an IS organization could protect RIM from budget or staffing cuts, assuming it is able to provide significant value to IS and the rest of the organization.

Perhaps even more importantly, the role of CISOs has been elevated because cyber threats are consistently seen as some of the greatest organizational risks. By aligning with someone so important in the organizational structure, RIM professionals could have more opportunities to:

- Articulate the importance of RIM to the organization
- Redefine, reposition, and expand their role within the organization
- Influence organizational strategy more directly
- Be seen as leaders themselves

Make the Pitch

An opportune time to champion re-positioning RIM within the organization's IS department is during reorganization. It may be difficult to anticipate such changes, though, so it is important to be proactive in preparing to advocate this change to leadership as opportunity allows.

First, develop a relationship with the CISO to determine whether he or she may be receptive to such a move. Begin developing expertise in the IS field so the CISO will see the value you bring to the organization when it is time to make the pitch.

Develop a proposal that outlines the benefits of this change to IS, RIM, and the organization as a whole. The key is articulating how shared expertise can enhance both functions. Also be sure to outline cost savings that can be gained from the move.

Look for an opportunity to present the proposal to the CISO; absent a reorganization or changes in leadership, a high-profile data breach in the news may stimulate a discussion taht could include the proposal.

If the proposal is ultimately rejected, view it as an opportunity to continue to develop the relationship and strategic alignment with IS, and look for ways to work together in future projects. Mutual success on specific projects may be the best evidence for an eventual reorganization. E

About the Author: Andrew Altepeter is a senior analyst, Information Security Governance, at Motorola Solutions, where he is responsible for records management, information security policy and standards, compliance, training, and awareness. He has a graduate degree in history and has previous experience in archives. Altepeter can be reached at *andrew.altepeter@gmail.com*.