Pursue **Privacy Roles** to Propel Your Career

April Dmytrenko, CRM, FAI

With the current hyper-focus on protecting information assets, this is an optimum time for records and information management professionals to leverage their commonalities with their privacy counterparts and expand their role – or even take the lead – in their organizations' privacy efforts.

Editor's Note: Welcome to the first Fellows Forum, which will appear in each issue of *Information Management* magazine to expand and provoke forward thinking about the records and information management (RIM) profession. Each article will be authored by a RIM professional who – through his or her outstanding achievements and contributions to RIM and to ARMA International at the local, regional, and national levels – has received the distinction of being named a Fellow of ARMA International (FAI). The Company of Fellows was established in 1990 and has 51 members worldwide.

Every year of my long and rich career in records and information management (RIM) has been more rewarding than the previous one, offering greater challenges and opportunities to expand my knowledge, experience, and sphere of influence.

Although the fundamental responsibility of RIM remains the management of the records and information lifecycle, the complex and sophisticated knowledge and experience required for a senior-level RIM professional today put the position on par with C-level executives in terms of their value to the organization.

The position has been elevated, fortunately or not, by the costly risks and severe consequences of litigation, non-compliance, and data breaches that organizations now face. From my perspective, and according to frequent news headlines, a data breach is one of the most threatening concerns.

When protected data is viewed, stolen, or used by unauthorized parties, there can be devastating repercussions, including damage to the organization's reputation and brand, loss of revenue, lawsuits and sanctions, lost customers, and negatively impacted company value.

Opportunity for RIM

The discipline of privacy, which is focused on the appropriate collection, use, access, protection, disposition, and overall governance of personal or other highly confidential/sensitive information, offers RIM professionals an additional avenue for expanding their role.

Taking on privacy responsibilities or serving in a key advisory role provide a golden opportunity to increase and demonstrate your value to your organization. There are many potential privacy roles from which to choose, such as privacy governance, cyber/data security, forensics and penetration testing, and breach/incident response – and new roles are continuing to emerge for both practitioners and service providers.

Program Similarities

RIM has crossed paths with privacy for decades due to their common information concerns. In fact, the RIM profession was the first to take accountability for protecting an organization's records and information. In the January 1967 *Records Management Quarterly* (this publication's predecessor), Association President Eunice M. Thompson emphasized information protection as one of the records profession's main responsibilities. (See Figure 1.)

A SPECIAL MEMO TO ARMA MEMBERS AND SUBSCRIBERS

I am very pleased to introduce to you the "*Records Management Quarterly*." As a successor to our association's previous publication, the *Records Review*, it represents for the American Records Management Association (ARMA) and the fields of records management an expanded means of promoting the many techniques and principles of sound records programming.

For the past ten years ARMA has attempted, through the *Review*, to serve the ever increasing need for business and industry knowledge on the subject of improved efficiency and economy in paperwork creation—processing—retention—retrieval—and protection. It is ARMA's primary objective to continue this service in its *Records Management Quarterly*.

Figure 1: Nearly a half-century ago, Association President Eunice M. Thompson emphasized information protection as one of the main responsibilities of the records profession. Source: *Records Management Quarterly*, Volume 1, No. 1, January 1967.

Today, the business- and legal-driven elements of RIM and privacy programs have connected the disciplines much more closely. While different in their specific objectives, many similarities exist, including the elements that follow.

Program Components

It is essential that both disciplines have the following key components to ensure legally compliant programs. At a high level, it is apparent how common the approaches to RIM and privacy are.

An information governance (IG) framework is essential for the success of both programs, and it must be sustained. This includes having senior management support, a designated point person to manage day-to-day activities, and an ongoing oversight or steering committee.

In this framework, all roles and responsibilities should be clearly defined. RIM and privacy professionals can be instrumental in serving on committees for business continuity and IT systems, as well as on each other's committees.

Specific to privacy, an incident response committee is instrumental to the timely support of a data breach. This role handles confirmation that a breach has actually occurred, containment, notification/communications (during and post-breach), and documentation of the cause and all actions taken.

Policies and procedures are necessary for both programs to ensure proper lifecycle management. We know clearly what this entails on the RIM side, but for privacy it outlines policies and procedures for the identification of protected information, the requirements for its safeguarding, and the management of any breaches.

The policies and procedures for both programs need to address all stakeholders. That includes not only employees, but the board of directors, contractors, and third parties, as they all are involved with records and information.

Policies and procedures must be outlined in third parties' contracts if they maintain records for their client organizations. Certainly, third parties need to follow each client's records retention schedule, and if they have a data breach, they need to know what is expected of them in notifying their client.

Communications and training are critical to both programs. Even with the best program, IG framework, and policies and procedures, an organization that fails on the communications and training component will not have a compliant approach. This requires an ongoing process with clear, concise messaging that builds awareness.

Specific to the privacy program, specialized training for breach pre-

paredness is important to ensure that emergency readiness is in place. Conducting *tabletop exercises*, which simulate emergency situations and allow personnel to practice the appropriate reactions in a relatively stress-free environment, can be very effective for preparing personnel.

Ongoing process improvements are imperative to ensure both programs' health and legal compliance. Both RIM and privacy are driven by an audit and compliance component to address myriad aspects, including identified issues, failures, opportunities for improvement, and new laws or regulations. Process improvements also address any business changes, such as business partners, information workflows and technology, acquisitions and divestitures, and geographic operations. The outcome could range from minor procedural changes to more substantial changes that require adding staff or budget.

Legal Requirements

Globally, there exist complex and ever-changing laws and regulations that impact both RIM and privacy.

RIM's scope includes all of an organization's records and information. A records retention schedule outlines, at a high level, categories specific to an organization and defines the legal retention requirements plus any additional time needed for business purposes.

Privacy's scope includes an organization's records that have been identified as containing PII and other confidential or sensitive information. There are legal recordkeeping requirements specifically for information containing PII, including for collecting, using, and disseminating it. There are also requirements for reporting data breach incidents.

Progressive RIM programs incorporate privacy laws and regulations into their records retention schedules, as well as the legal requirements.

Figure 2. Generally Accepted Best Practices Principles

Best Practices Alignment

Each of the disciplines has formal principles to help organizations develop and manage effective programs. RIM has the Generally Accepted Recordkeeping Principles® developed by ARMA International. The privacy profession follows the Generally Accepted Privacy Principles developed by the AICPA/CICA Privacy Task Force, a joint task force of the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

As shown by Figure 2, "Generally Accepted Best Practices" Principles, even though the terminology and some of the perspectives are not identical, these principles align, providing yet another commonality upon which RIM and privacy professionals can collaborate.

Privacy Careers

With today's tremendous focus on records and information, RIM professionals have immense value to their organization's privacy efforts, in terms of their:

- Expertise in information lifecycle management
- Knowledge about the organization's business environment
- Collaborative relationships with key stakeholders in corporate groups such as IT, legal, human resources, audit, and business units
- Enterprise-wide oversight
- Accountability for ensuring legally compliant practices

For these reasons, RIM and privacy are beginning to be integrated in 1) positions that combine the two disciplines, 2) in reporting relationships, and 3) in RIM career paths that are expanding to include privacy leadership. RIM aligning with privacy and vice versa are not just a matter of desire.

Although the privacy discipline is complex, challenging, and always evolving, there is a tremendous amount of information available for RIM professionals who want or need to expand their knowledge.

ARMA International continues to have a growing focus on the topic

Evolution of the Privacy Concept

The concept of privacy may seem a relatively new one, but it dates back to some of the oldest cultures and is referenced in the Bible and Quran. It continued to develop slowly throughout the world as part of the legal-based protections around *personal* privacy as it relates to freedom from being watched or spied on. In 1361, for example, England enacted provisions that called for the arrest of peeping toms and eavesdroppers.

Personal privacy protection continued to evolve into personal *information* protection as we know it today. In 1858, France started issuing strict fines for those publishing others' private information. In the United States, the *Harvard Law Review* published an article in 1890 titled "The Right to Privacy," which is widely regarded as the first U.S. publication to advocate that right. This was driven by privacy concerns over increasing coverage of scandals in newspapers and the advent of consumer hand-held cameras that could take candid pictures. Ironically, these same concerns exist today.

Fast forward to the 20th century with the emergence of information technology, its rapid development, and the acceleration of capturing, analyzing, sharing, and using data. Largely as a result of this, as well as the egregious use of personal information during World War II, our global information economy drove privacy laws.

These laws protect a wide variety of personal information, including any personally identifiable information (PII), such as medical, credit card, and student loan information. They also address the collection, handling, and use of this information, such as unlawful seizure, transfer outside certain borders, and selling without the data subject's consent.

of privacy in its wide variety of educational offerings and published materials.

The International Association of Privacy Professionals, which is recognized globally in the privacy community, has a wealth of information on its website and in its publications, conferences/workshops, networking opportunities, and certifications. There are even more resources available to its members.

Law firms that specialize in privacy usually offer free privacy law blogs, news briefs, and webinars.

Privacy consulting, service, and technology firms offer a variety of white papers, industry reports, data sheets, and webinars.

Privacy insurance firms offer cyber risk news briefs, newsletters, and industry information.

Government agencies offer a wide range of information, including articles, regarding laws and regulations.

Time to Engage

RIM has never been more important to the business world. With so much focus on the management and protection of information assets, there are tremendous opportunities for RIM professionals to become more involved – even take the lead – in their organizations' privacy efforts. At the least, they should strive to complement, support, and integrate privacy elements into their work, language, and programs. The RIM and privacy paths are connected; RIM and privacy professionals now must engage to achieve their common goals. **END**

April Dmytrenko, CRM, FAI, can be contacted at ADmytrenko2@aol.com. *See her bio on page 47.*